P-2812HNU-51c

Dual WAN VDSL2 IAD with 802.11n Wireless

User's Guide

Default Login Details

IP Address	192.168.1.1
User Name	Admin account: admin User account: user
Password	Admin account: 1234 User account: user

Firmware Version 1.02
Edition 1, 06/2010

ZyXEL

www.zyxel.com

Copyright © 2010
ZyXEL Communications Corporation

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the P-2812HNU-51c using the web configurator.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Support Disc

  Refer to the included CD for support documents.

Documentation Feedback

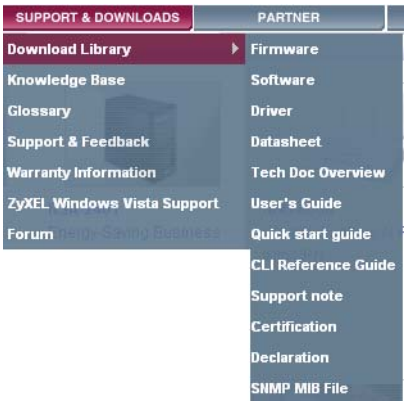
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

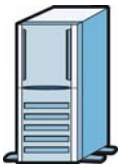
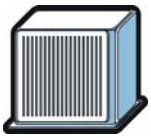
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-2812HNU-51c may be referred to as the "P-2812HNU-51c", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The P-2812HNU-51c icon is not an exact representation of your device.

P-2812HNU-51c	Computer	Notebook computer
Server 	DSLAM 	Firewall
Telephone	Switch	Router

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

User's Guide 21

Introducing the P-2812HNU-51c 23
Tutorials 33
Introducing the Web Configurator 73

Technical Reference 79

Status Screens 81
WAN Setup 97
LAN Setup 137
Wireless LAN 149
Network Address Translation (NAT) 183
Voice 195
File Sharing 233
Sharing a USB Printer 239
IPSec VPN 253
Firewall 275
Certificate 281
Static Route 293
Policy Forwarding 297
DNS Route 301
RIP 305
Quality of Service (QoS) 307
Dynamic DNS Setup 329
Remote Management 331
Universal Plug-and-Play (UPnP) 339
Parental Control 349
Interface Group 353
E-mail Notification 359
System Settings 363
Logs 367
Tools 371
Diagnostic 379
Troubleshooting 385
Product Specifications 395

Table of Contents

About This User's Guide 3

Document Conventions 5

Safety Warnings 7

Contents Overview 9

Table of Contents 11

Part I: User's Guide 21

Chapter 1
Introducing the P-2812HNU-51c 23

1.1 Overview 23
1.2 Ways to Manage the P-2812HNU-51c 24
1.3 Good Habits for Managing the P-2812HNU-51c 24
1.4 Applications for the P-2812HNU-51c 24
1.4.1 Internet Access 24
1.4.2 VoIP Internet Calls 27
1.4.3 USB File Sharing 27
1.4.4 Wireless Connection 28
1.5 The RESET Button 29
1.5.1 Using the Reset Button 29
1.6 LEDs (Lights) 30

Chapter 2
Tutorials 33

2.1 Overview 33
2.2 How to Set up a Wireless Network 33
2.2.1 Example Parameters 33
2.2.2 Configuring the AP 34
2.2.3 Configuring the Wireless Client 36
2.3 How to Use ATM QoS with Multiple PVCs and Interface Groups 43
2.3.1 Configuring PVCs 44
2.3.2 Setting Interface Groups 53
2.3.3 Configuring Interface Group IP 57
2.3.4 Testing the DSL Connection Groups 59

2.4 How to Allow Out-of-band Remote Management from the WAN 60
2.4.1 Configuring Multiple WAN Connections 60
2.4.2 Configuring Remote Management 70
2.4.3 Testing the Connection 71

Chapter 3
Introducing the Web Configurator 73

3.1 Web Configurator Overview 73
3.1.1 Accessing the Web Configurator 73
3.2 Web Configurator Main Screen 74
3.2.1 Navigation Panel 75
3.2.2 Main Window 78
3.2.3 Status Bar 78

Part II: Technical Reference 79

Chapter 4
Status Screens 81

4.1 Overview 81
4.2 Status Screen 82
4.2.1 3G Status: NeedPIN 87
4.2.2 3G Status: NeedPUK 88
4.2.3 WAN Service Statistics 89
4.2.4 Route Info 90
4.3 VoIP Status 92
4.3.1 WLAN Station List 94
4.3.2 LAN Statistics 95
4.3.3 Client List 96

Chapter 5
WAN Setup 97

5.1 Overview 97
5.1.1 What You Can Do in this Chapter 97
5.2 What You Need to Know 99
5.3 Before You Begin 101
5.4 The Layer 2 Interface Screen 101
5.4.1 Layer 2 Interface Configuration 102
5.5 The Internet Connection Screen 105
5.5.1 Internet Connection Configuration 107
5.6 The 3G Backup Screen 122
5.7 Technical Reference 125

Chapter 6
LAN Setup 137

6.1 Overview 137
6.1.1 What You Can Do in this Chapter 137
6.2 What You Need To Know 138
6.3 The LAN IP Screen 139
6.4 The LAN IPv6 Screen 142
6.5 Technical Reference 143

Chapter 7
Wireless LAN 149

7.1 Overview 149
7.1.1 What You Can Do in this Chapter 149
7.2 What You Need to Know 150
7.3 Before You Begin 152
7.4 The General Screen 153
7.4.1 No Security 155
7.4.2 WEP Encryption 156
7.4.3 WPA(2)-PSK 157
7.4.4 WPA(2) Authentication 158
7.4.5 MAC Filter 160
7.4.6 Adding a New MAC Filtering Rule 161
7.5 The More AP Screen 162
7.5.1 More AP Edit 163
7.6 The WPS Screen 163
7.7 The WPS Station Screen 165
7.8 The WDS Screen 166
7.9 The Wireless Scheduling Screen 167
7.9.1 Adding a WLAN Power-off Scheduling Rule 169
7.10 The Advanced Setup Screen 170
7.11 Technical Reference 171
7.11.1 Wireless Network Overview 172
7.11.2 Additional Wireless Terms 173
7.11.3 Wireless Security Overview 173
7.11.4 WiFi Protected Setup 175

Chapter 8
Network Address Translation (NAT) 183

8.1 Overview 183
8.1.1 What You Can Do in this Chapter 183
8.2 What You Need to Know 183
8.3 The Port Forwarding Screen 184
8.3.1 The Port Forwarding Edit Screen 186

8.4 The Trigger Port Screen 187
8.4.1 Trigger Port Configuration 190
8.5 The DMZ Host Screen 192
8.6 The ALG Screen 192
8.7 Technical Reference 193

Chapter 9
Voice 195

9.1 Overview 195
9.1.1 What You Can Do in this Chapter 195
9.1.2 What You Need to Know About VoIP 196
9.2 Before You Begin 197
9.3 The SIP Settings Screen 197
9.4 The SIP Service Provider Screen 203
9.4.1 Dial Plan Rules 210
9.5 The Phone Region Screen 211
9.6 The Speed Dial Screen 212
9.7 Call History Summary Screen 214
9.8 Outgoing Calls Screen 215
9.9 Incoming Calls Screen 216
9.10 Technical Reference 216
9.10.1 Quality of Service (QoS) 225
9.10.2 Phone Services Overview 227

Chapter 10
File Sharing 233

10.1 Overview 233
10.1.1 What You Can Do in this chapter 233
10.1.2 What You Need to Know 234
10.1.3 Before You Begin 235
10.2 The File Sharing Screen 236
10.2.1 Example of Accessing Your Shared Files From a Computer 237

Chapter 11
Sharing a USB Printer 239

11.1 Overview 239
11.1.1 What You Can Do in this chapter 239
11.2 What You Need to Know 240
11.3 Before You Begin 240
11.4 The Print Server Screen 241
11.5 Add a New Printer Using Windows 242
11.6 Add a New Printer Using Macintosh OS X 245
11.6.1 Mac OS 10.3 and 10.4 245

11.6.2 Mac OS 10.5 and 10.6 248
11.7 P-2812HNU-51c Print Server Compatible USB Printers 252

Chapter 12
IPSec VPN 253

12.1 Overview 253
12.1.1 What You Can Do in this Chapter 253
12.2 What You Need to Know 254
12.2.1 Before You Begin 255
12.3 The IPSec Screen 255
12.3.1 The IPSec Setting Screen 256
12.3.2 Manual Key Setup 261
12.3.3 Configuring Manual Key 262
12.4 Viewing VPN Status 266
12.5 IPSec VPN Technical Reference 267
12.5.1 IPSec Architecture 267
12.5.2 Encapsulation 268
12.5.3 IKE Phases 269
12.5.4 Negotiation Mode 270
12.5.5 IPSec and NAT 270
12.5.6 VPN, NAT, and NAT Traversal 271
12.5.7 ID Type and Content 272
12.5.8 Pre-Shared Key 274
12.5.9 Diffie-Hellman (DH) Key Groups 274

Chapter 13
Firewall 275

13.1 Overview 275
13.1.1 What You Can Do in this Chapter 275
13.2 What You Need to Know 275
13.3 The Firewall Screen 276
13.3.1 Creating Incoming Firewall Rules 278

Chapter 14
Certificate 281

14.1 Overview 281
14.1.1 What You Can Do in this Chapter 281
14.2 What You Need to Know 281
14.3 The Local Certificates Screen 282
14.3.1 Create Certificate Request 283
14.3.2 Import Certificate 284
14.3.3 Certificate Details 286
14.3.4 Load Signed Certificate 288

14.4 The Trusted CA Screen 289
14.4.1 View Trusted CA Certificate 291
14.4.2 Import Trusted CA Certificate 292

Chapter 15
Static Route 293

15.1 Overview 293
15.1.1 What You Can Do in this Chapter 293
15.2 The Static Route Screen 294
15.2.1 Static Route Edit 295

Chapter 16
Policy Forwarding 297

16.1 Overview 297
16.1.1 What You Can Do in this Chapter 297
16.2 The Static Route Screen 297
16.2.1 Policy Forwarding Setup 298

Chapter 17
DNS Route 301

17.1 Overview 301
17.1.1 What You Can Do in this Chapter 302
17.2 The DNS Route Screen 302
17.2.1 DNS Route Edit 303

Chapter 18
RIP 305

18.1 Overview 305
18.1.1 What You Can Do in this Chapter 305
18.2 The RIP Screen 305

Chapter 19
Quality of Service (QoS) 307

19.1 Overview 307
19.1.1 What You Can Do in this Chapter 307
19.2 What You Need to Know 308
19.3 The Quality of Service General Screen 309
19.4 The Queue Setup Screen 311
19.4.1 Adding a QoS Queue 312
19.5 The Class Setup Screen 313
19.5.1 QoS Class Edit 315
19.6 The QoS Policer Setup Screen 319
19.6.1 Adding a QoS Policer 320

19.7 The QoS Monitor Screen 323
19.8 Technical Reference 324

Chapter 20
Dynamic DNS Setup 329

20.1 Overview 329
20.1.1 What You Can Do in this Chapter 329
20.2 What You Need To Know 329
20.3 The Dynamic DNS Screen 330

Chapter 21
Remote Management 331

21.1 Overview 331
21.1.1 What You Can Do in this Chapter 331
21.2 The TR-069 Screen 331
21.3 The TR-064 Screen 333
21.4 The SNMP Screen 334
21.5 The Service Control Screen 336
21.6 The IP Address Screen 337
21.6.1 Adding an IP Address 338

Chapter 22
Universal Plug-and-Play (UPnP) 339

22.1 Overview 339
22.1.1 What You Can Do in this Chapter 339
22.2 What You Need to Know 339
22.3 The UPnP Screen 340
22.4 Installing UPnP in Windows 341
22.4.1 Windows 7 341
22.4.2 Windows XP 342
22.5 Using UPnP in Windows XP 343
22.5.1 Auto-discover Your UPnP-enabled Network Device 344
22.5.2 Web Configurator Easy Access 346

Chapter 23
Parental Control 349

23.1 Overview 349
23.1.1 What You Can Do in this Chapter 349
23.2 The Time Restriction Screen 349
23.2.1 Adding a Schedule 350
23.3 The URL Filter Screen 351
23.3.1 Adding URL Filter 352

Chapter 24
Interface Group 353

24.1 Overview 353
24.1.1 What You Can Do in this Chapter 353
24.2 The Interface Group Screen 353
24.2.1 Interface Group Configuration 355
24.2.2 Interface Grouping Criteria 356

Chapter 25
E-mail Notification 359

25.1 Overview 359
25.1.1 What You Can Do in this Chapter 359
25.2 The Email Notification Screen 359
25.2.1 Email Notification Edit 360

Chapter 26
System Settings 363

26.1 Overview 363
26.1.1 What You Can Do in this Chapter 363
26.2 The General Screen 363
26.3 The Time Setting Screen 364

Chapter 27
Logs 367

27.1 Overview 367
27.1.1 What You Can Do in this Chapter 367
27.2 The View Log Screen 367
27.3 The Log Settings Screen 368

Chapter 28
Tools 371

28.1 Overview 371
28.1.1 What You Can Do in this Chapter 371
28.2 The Firmware Screen 372
28.3 The Configuration Screen 374
28.4 The Restart Screen 376

Chapter 29
Diagnostic 379

29.1 Overview 379
29.1.1 What You Can Do in this Chapter 379
29.2 What You Need to Know 379
29.3 The General Diagnostic Screen 380

29.4 The 802.1ag Screen 381
29.5 The OAM Ping Test Screen 383

Chapter 30
Troubleshooting 385

30.1 Power, Hardware Connections, and LEDs 385
30.2 P-2812HNU-51c Access and Login 386
30.3 Internet Access 388
30.4 Phone Calls and VoIP 391
30.5 USB Device Connection 391
30.6 Wireless LAN Troubleshooting 392
30.7 UPnP 392

Chapter 31
Product Specifications 395

31.1 Hardware Specifications 395
31.2 Firmware Specifications 396

Appendix A Network Troubleshooting 401

Appendix B Setting Up Your Computer's IP Address 417

Appendix C Pop-up Windows, JavaScripts and Java Permissions 445

Appendix D IP Addresses and Subnetting 455

Appendix E Wireless LANs 467

Appendix F IPv6 483

Appendix G Common Services 493

Appendix H Open Software Announcements 497

Appendix I Legal Information 511

Index 515

PART I
User's Guide

1

Introducing the P-2812HNU-51c

1.1 Overview

The P-2812HNU-51c is a VDSL2 Integrated Access Device (IAD) that combines a VDSL2+ router with Voice over IP (VoIP) communication capabilities. You may access the Internet in one of these ways:

- You can have super-fast, secure Internet access over analog (POTS) telephone lines. The P-2812HNU-51c supports both Packet Transfer Mode (PTM) and Asynchronous Transfer Mode (ATM) and can be backward compatible with ADSL, ADSL2 and ADSL2+.
- You can use an Ethernet WAN port for Internet access through the Ethernet WAN connection.
- You can use 3G as your WAN and access the Internet via a 3G network.

The P-2812HNU-51c also allows you to use a traditional analog telephone to make Internet calls. You can use Quality of Service (QoS) to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers.

Please refer to the following description of the product name format.

- “H” denotes an integrated 4-port hub (switch).
- “N” denotes IEEE 802.11n wireless functionality. There is an embedded mini-PCI module for IEEE 802.11b/g/n wireless LAN connectivity.
- “U” denotes a USB port used to set up a 3G WAN connection via a 3G wireless card or share files via a USB memory stick or a USB hard drive. The P-2812HNU-51c can also function as a print server with an USB printer connected.

Only use firmware for your P-2812HNU-51c’s specific model. Refer to the label on the bottom of your P-2812HNU-51c.

Models ending in “1”, for example P-2812HNU-51c, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service).

See Chapter 31 on page 395 for a full list of features.

1.2 Ways to Manage the P-2812HNU-51c

Use any of the following methods to manage the P-2812HNU-51c.

- Web Configurator. This is recommended for everyday management of the P-2812HNU-51c using a (supported) web browser.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 Good Habits for Managing the P-2812HNU-51c

Do the following things regularly to make the P-2812HNU-51c more secure and to manage the P-2812HNU-51c more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the P-2812HNU-51c to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the P-2812HNU-51c. You could simply restore your last configuration.

1.4 Applications for the P-2812HNU-51c

Here are some example uses for which the P-2812HNU-51c is well suited.

1.4.1 Internet Access

You can have up to eight WAN services over one ADSL, VDSL or Ethernet WAN line. The P-2812HNU-51c cannot work in ADSL, VDSL and Ethernet WAN mode at the same time.

Computers can connect to the P-2812HNU-51c's LAN ports (or wirelessly).

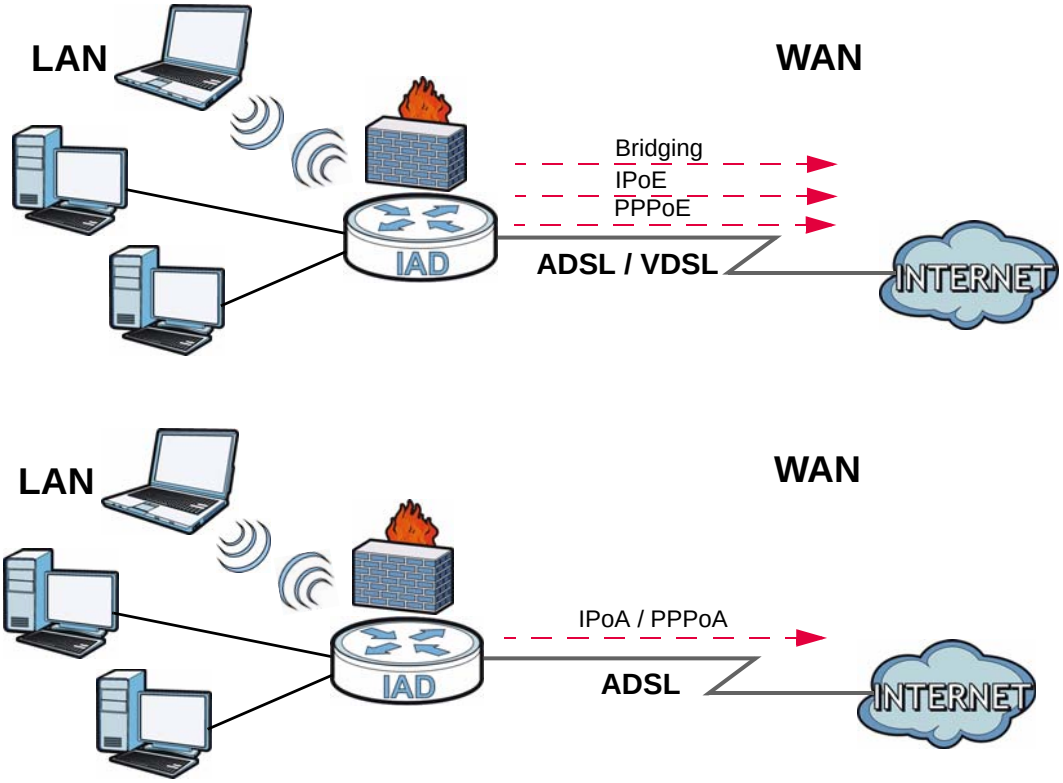
You can also configure IP filtering on the P-2812HNU-51c for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your

network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

1.4.1.1 DSL

Your P-2812HNU-51c provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack.

Figure 1 Internet Access Application: DSL

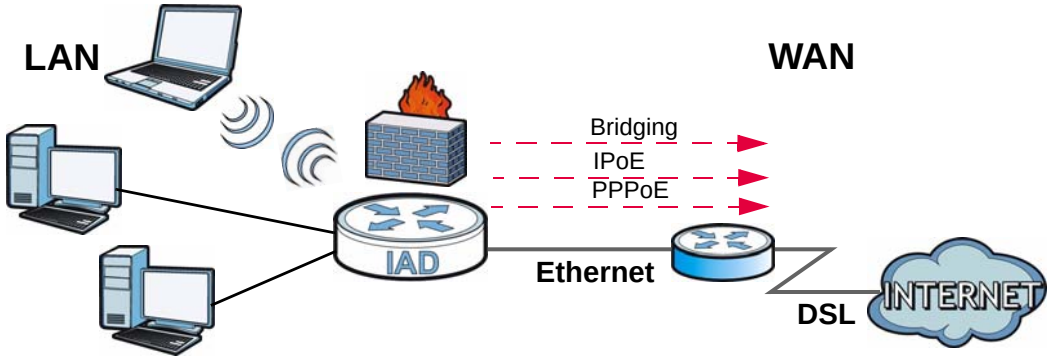


1.4.1.2 Ethernet WAN

If you prefer not to use a DSL line and you have another broadband modem or router (such as ADSL) available, you can push the **DSL / WAN** switch (on the rear panel) to the **WAN** side and connect the **WAN** port to the broadband modem or

router. This way, you can access the Internet via an Ethernet connection and still use the QoS, Firewall and VoIP functions on the P-2812HNU-51c.

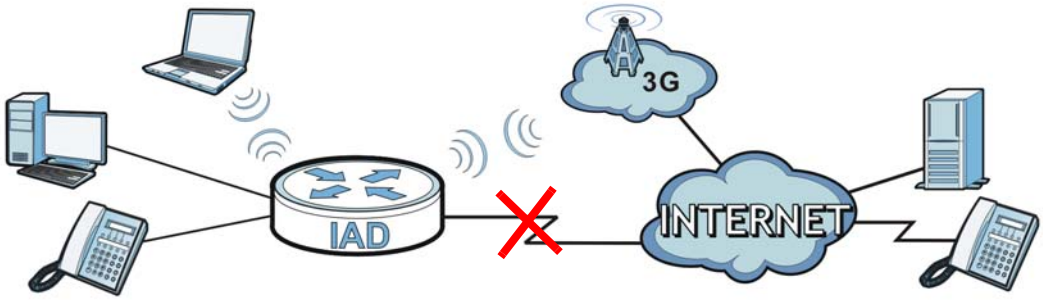
Figure 2 Internet Access Application: Ethernet WAN



1.4.1.3 3G WAN

The USB port allows you to wirelessly connect to a 3G netowk to get Internet access by attaching a 3G wireless card. You must leave the DSL or Ethernet WAN port unconnected and attached a 3G wireless card to use 3G as your WAN. You can also heve the P-2812HNU-51c use the 3G WAN connection as a backup. That means the P-2812HNU-51c switches to the 3G wireless WAN connection after the wired DSL or Ethernet WAN connection fails. The P-2812HNU-51c automatically changes back to use the wired DSL or Ethernet WAN connection when it is available.

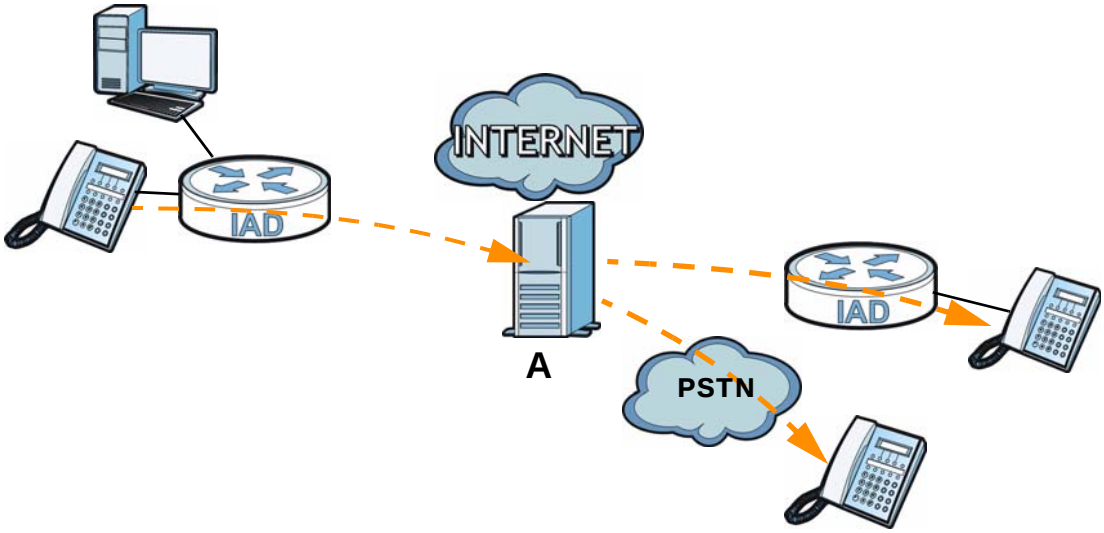
Figure 3 Internet Access Application: 3G WAN



1.4.2 VoIP Internet Calls

You can register up to two SIP (Session Initiation Protocol) accounts and use the P-2812HNU-51c to make and receive VoIP telephone calls:

Figure 4 P-2812HNU-51c's VoIP Application

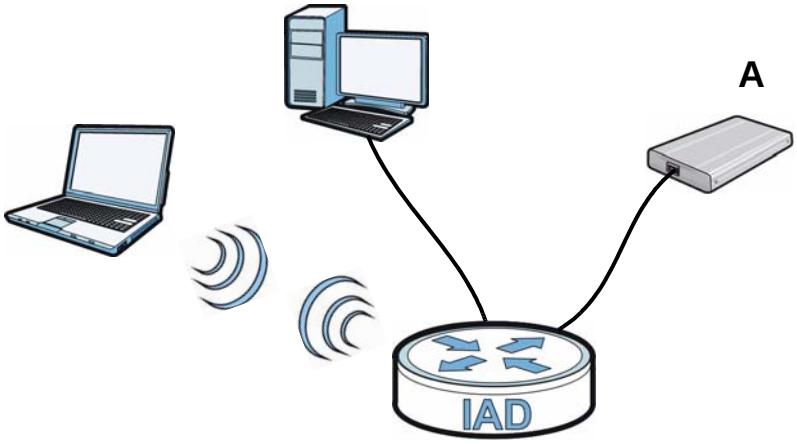


- Calls via a VoIP service provider (**A**) - The P-2812HNU-51c sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

1.4.3 USB File Sharing

Use the built-in USB 2.0 ports to share files via a USB memory stick or a USB hard drive (**A**). You can connect one USB hard drive to the P-2812HNU-51c at a time.

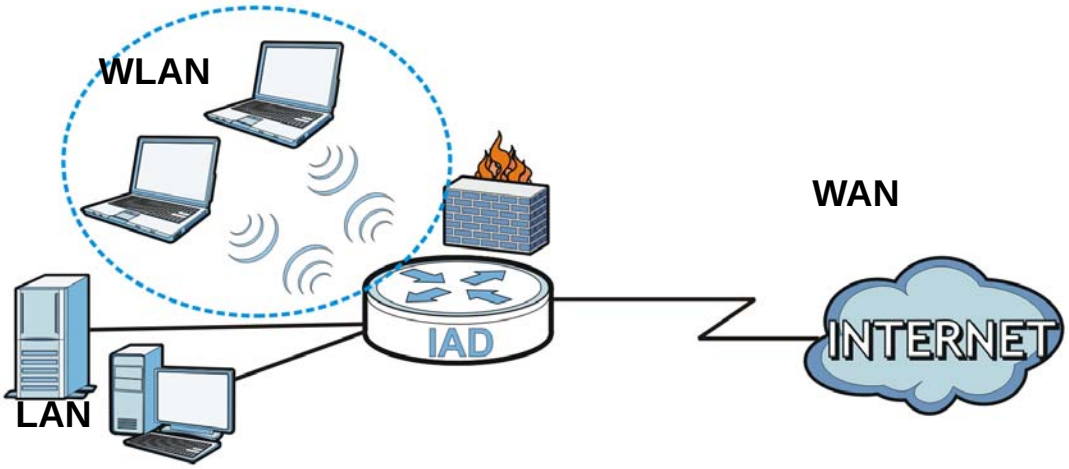
Figure 5 USB File Sharing Application



1.4.4 Wireless Connection

By default, the wireless LAN (WLAN) is enabled on the P-2812HNU-51c. IEEE 802.11a/b/g/n compliant clients can wirelessly connect to the P-2812HNU-51c to access network resources. You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

Figure 6 Wireless Connection Application



1.4.4.1 The WPS Button

You can use the **WPS** button on the rear panel of the device to turn the wireless LAN off or on. You can also use it to activate WPS in order to quickly set up a wireless network with strong security.

Turn the Wireless LAN Off or On

1. Make sure the **POWER** LED is on (not blinking).
2. Press the **WPS** button for one second and release it. The **WLAN / WPS** LED should change from on to off or vice versa.

Activate WPS

1. Make sure the **POWER** LED is on (not blinking).
2. Press the **WPS** button for more than five seconds and release it. Press the WPS button on another WPS -enabled device within range of the P-2812HNU-51c. The **WLAN / WPS** LED should flash while the P-2812HNU-51c sets up a WPS connection with the wireless device.

Note: You must activate WPS in the P-2812HNU-51c and in another wireless device within two minutes of each other. See Section 7.11.4 on page 175 for more information.

1.5 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”.

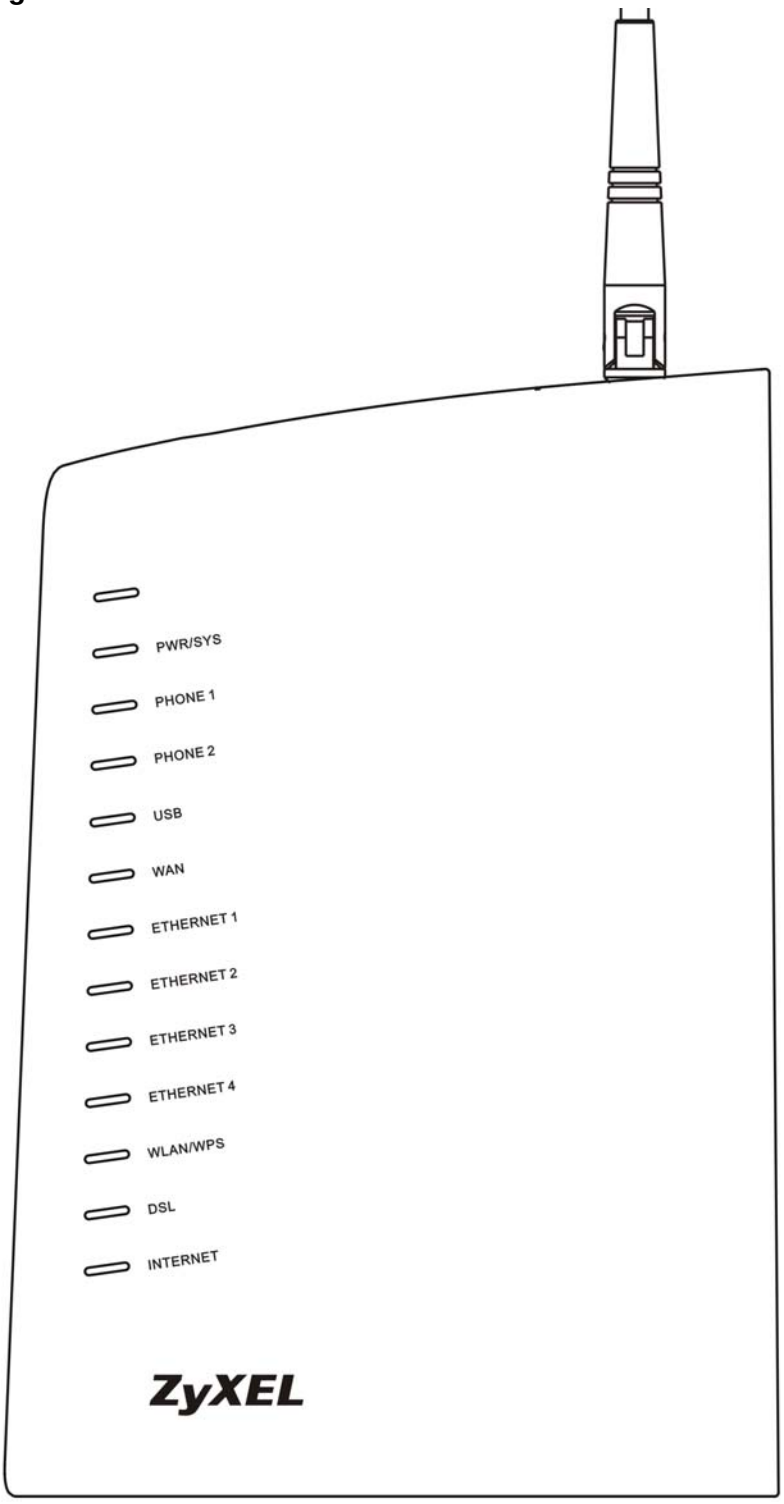
1.5.1 Using the Reset Button

1. Make sure the **POWER** LED is on (not blinking).
2. To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 7 LEDs on the Device



None of the LEDs are on if the P-2812HNU-51c is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Green	On	The P-2812HNU-51c is receiving power and ready for use.
		Blinking	The P-2812HNU-51c is self-testing.
	Red	On	The P-2812HNU-51c detected an error while self-testing, or there is a device malfunction.
		Off	The P-2812HNU-51c is not receiving power.
PHONE 1/2	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Orange	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account.
		Off	The phone port does not have a SIP account registered.
USB	Green	On	The P-2812HNU-51c recognizes a USB connection.
		Blinking	The P-2812HNU-51c is sending/receiving data to /from the USB device connected to it.
		Off	The P-2812HNU-51c does not detect a USB connection.
WAN	Green	On	The P-2812HNU-51c has an Ethernet connection with a device on the WAN.
		Blinking	The P-2812HNU-51c is sending/receiving data to/from the WAN.
		Off	The P-2812HNU-51c does not have an Ethernet connection with the WAN.
ETHERNET 1-4	Green	On	The P-2812HNU-51c has a successful 1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The P-2812HNU-51c is sending or receiving data to/from the LAN at 1000 Mbps.
	Orange	On	The P-2812HNU-51c has a successful 10/100 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The P-2812HNU-51c is sending or receiving data to/from the LAN at 10/100 Mbps.
		Off	The P-2812HNU-51c does not have an Ethernet connection with the LAN.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
WLAN/ WPS	Green	On	The wireless network is activated and is operating in IEEE 802.11b/g mode.
		Blinking	The P-2812HNU-51c is communicating with other wireless clients.
	Orange	Blinking	The P-2812HNU-51c is setting up a WPS connection.
		Off	The wireless network is not activated.
DSL	Green	On	The ADSL line is up.
		Blinking	The P-2812HNU-51c is initializing the ADSL line.
	Orange	On	The VDSL line is up.
		Blinking	The P-2812HNU-51c is initializing the VDSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The P-2812HNU-51c has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The P-2812HNU-51c is sending or receiving IP traffic.
	Red	On	The P-2812HNU-51c attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The P-2812HNU-51c does not have an IP connection.

Refer to the Quick Start Guide for information on hardware connections.

2

Tutorials

2.1 Overview

This chapter describes:

- How to Set up a Wireless Network on page 33.
- How to Use ATM QoS with Multiple PVCs and Interface Groups on page 43.
- How to Allow Out-of-band Remote Management from the WAN on page 60.

Note: The tutorials featured in this chapter require a basic understanding of connecting to and using the Web Configurator on your P-2812HNU-51c. For details, see the included Quick Start Guide. For field descriptions of individual screens, see the related technical reference in this User's Guide.

2.2 How to Set up a Wireless Network

This tutorial gives you examples of how to set up an access point and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through an AP wirelessly.

2.2.1 Example Parameters

SSID	SSID_Example3
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	IEEE 802.11b/g/n Mixed

An access point (AP) or wireless router is referred to as “AP” and a computer with a wireless network card or USB/PCI adapter is referred to as “wireless client” here.

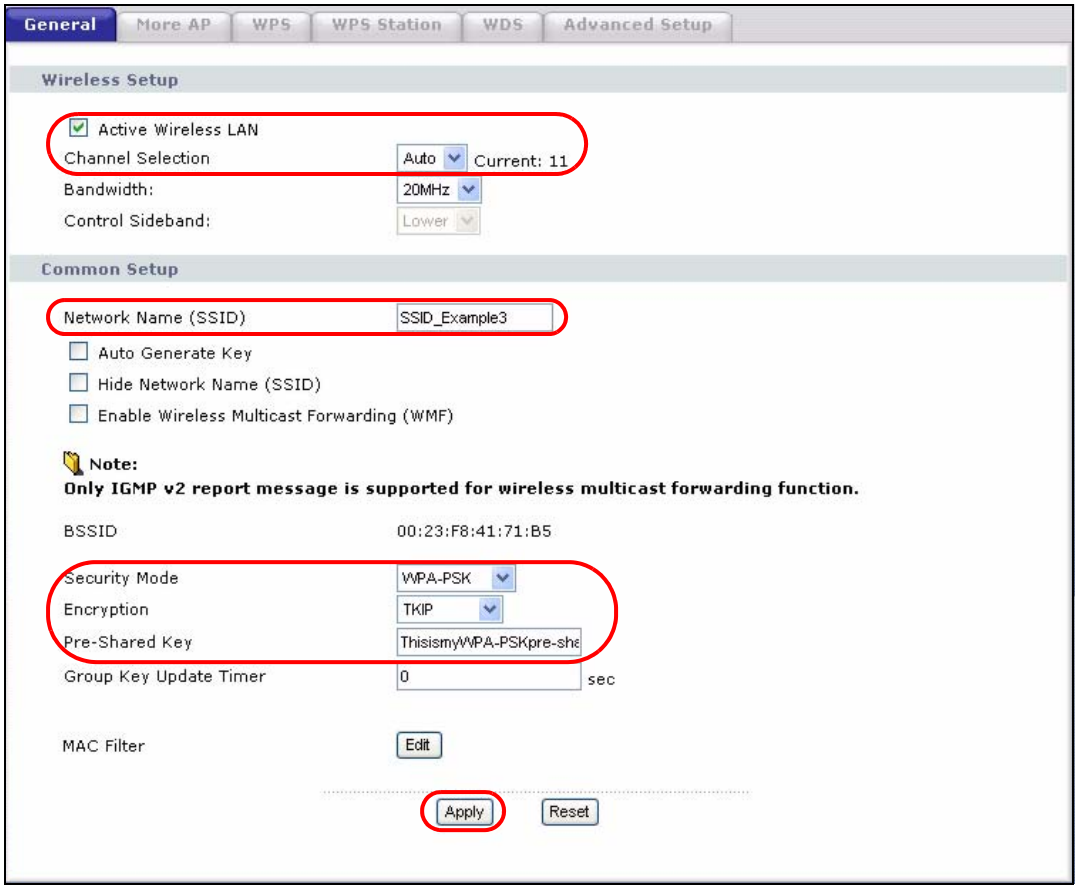
We use the P-2812HNU-51c web screens and M-302 utility screens as an example. The screens may vary slightly for different models.

2.2.2 Configuring the AP

Follow the steps below to configure the wireless settings on your AP.

1 Open the **Network > Wireless LAN** screen in the AP's web configurator.

Figure 8 AP: Wireless LAN



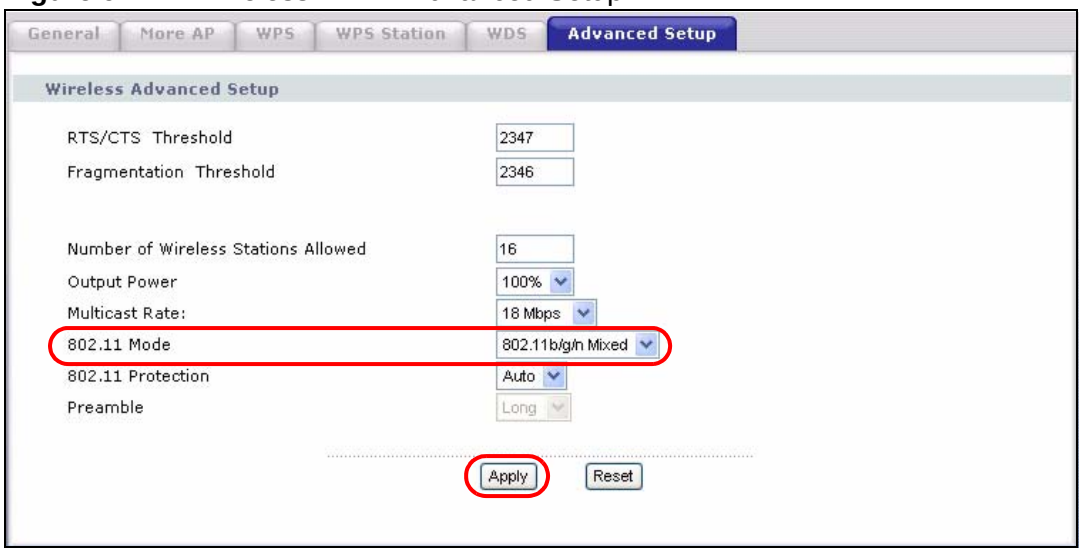
2 Make sure the **Active Wireless LAN** check box is selected.

3 Enter "SSID_Example3" as the SSID and select **Auto** to have the P-2812HNU-51c automatically determine a channel which is not used by another AP.

4 Set security mode to **WPA-PSK** and enter "ThisismyWPA-PSKpre-sharedkey" in the **Pre-Shared Key** field. Click **Apply**.

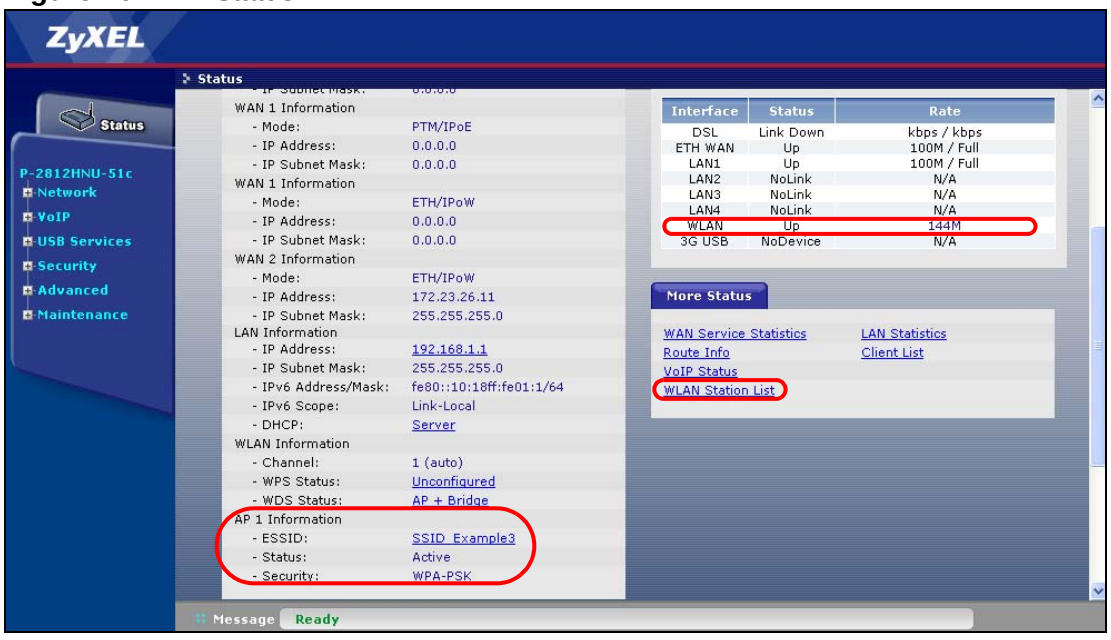
5 Click the **Advanced Setup** tab and select **802.11b/g/n Mixed** in the **802.11 Mode** field. Click **Apply**.

Figure 9 AP: Wireless LAN > Advanced Setup



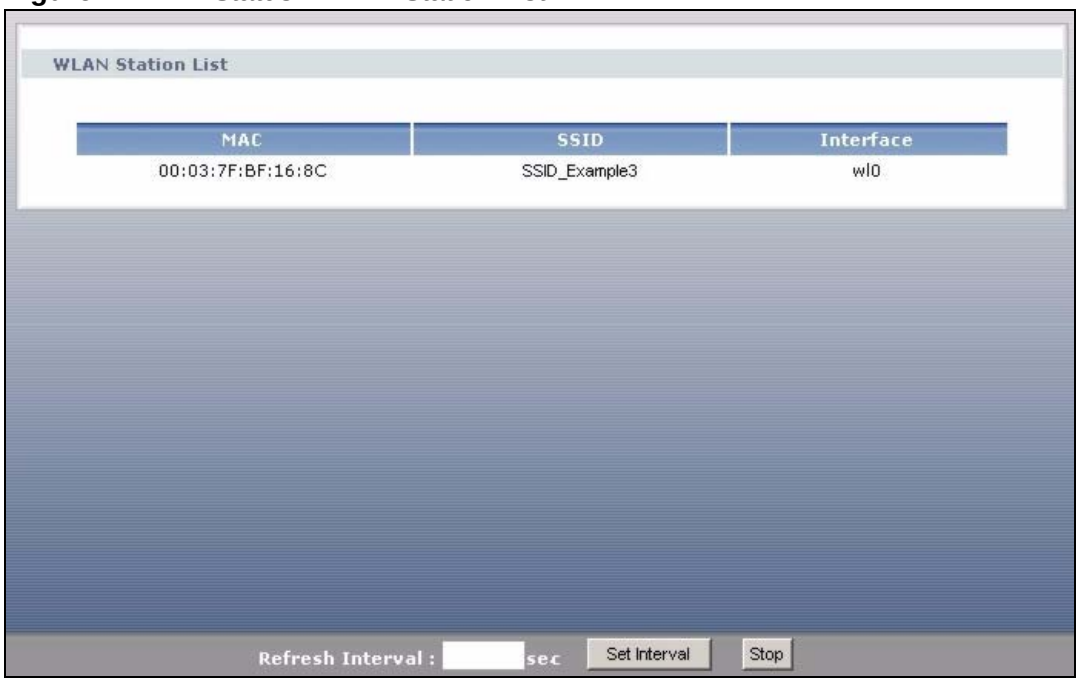
6 Open the **Status** screen.Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 10 AP: Status



7 Click the **WLAN Station List** hyperlink in the AP's **Status** screen. You can see if any wireless client has connected to the AP.

Figure 11 AP: Status: WLAN Station List



2.2.3 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

2.2.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.

C **AP**

There are three ways to connect the client to an access point.

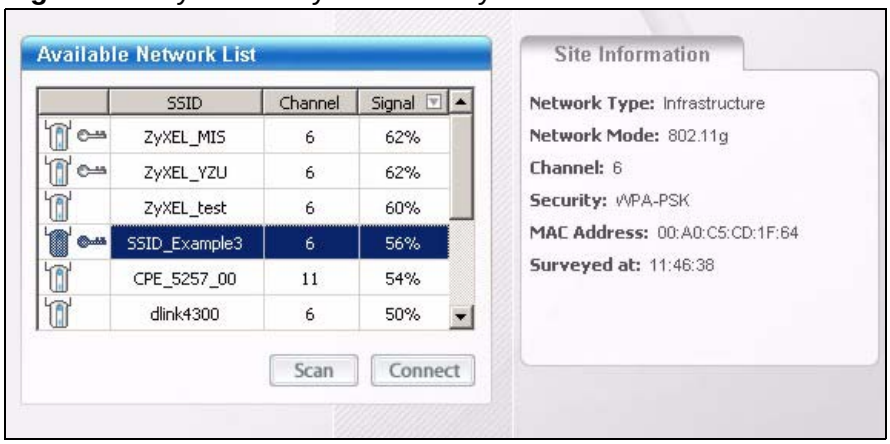
- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is “SSID_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”.

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

Figure 12 ZyXEL Utility: Site Survey

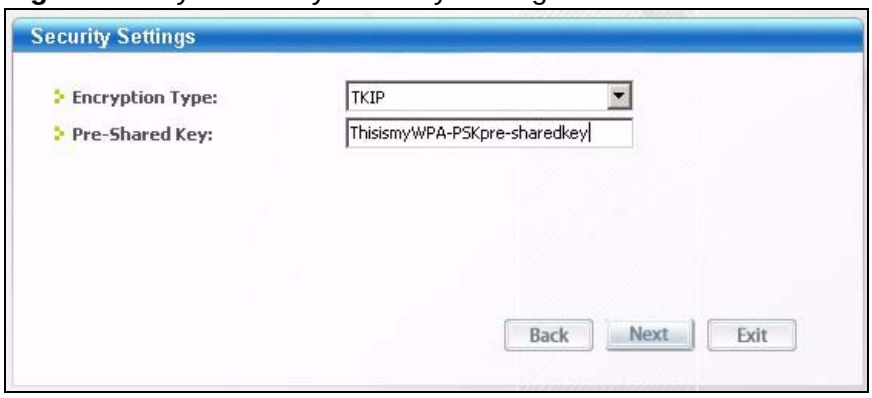


2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.

3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

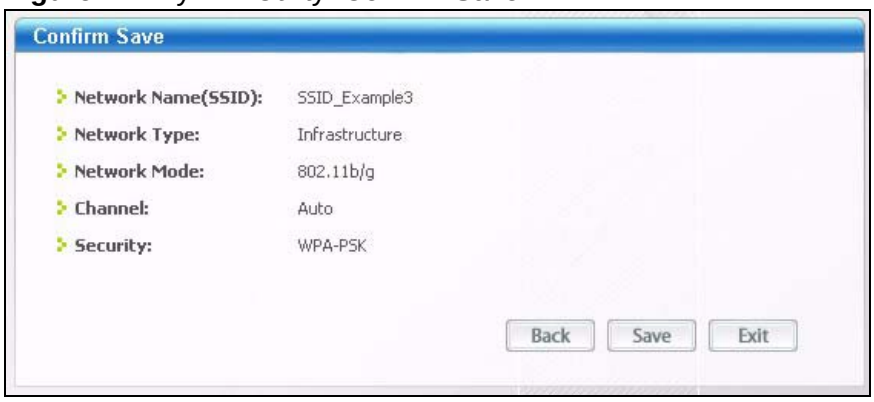
Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

Figure 13 ZyXEL Utility: Security Settings



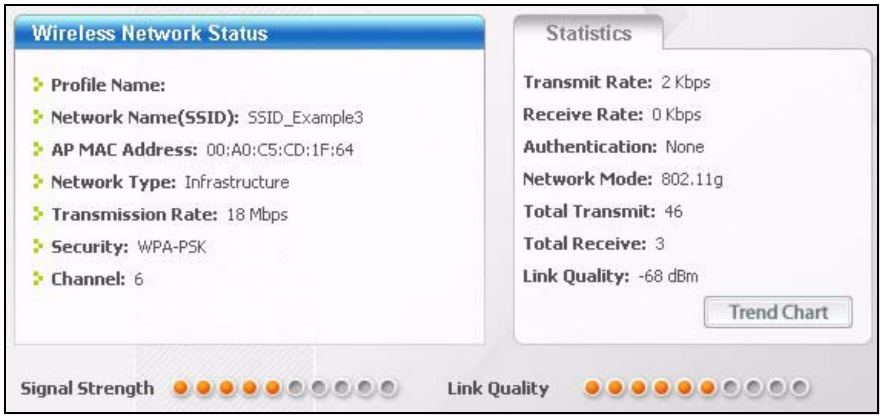
4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 14 ZyXEL Utility: Confirm Save



5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.

Figure 15 ZyXEL Utility: Link Info



6 Open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

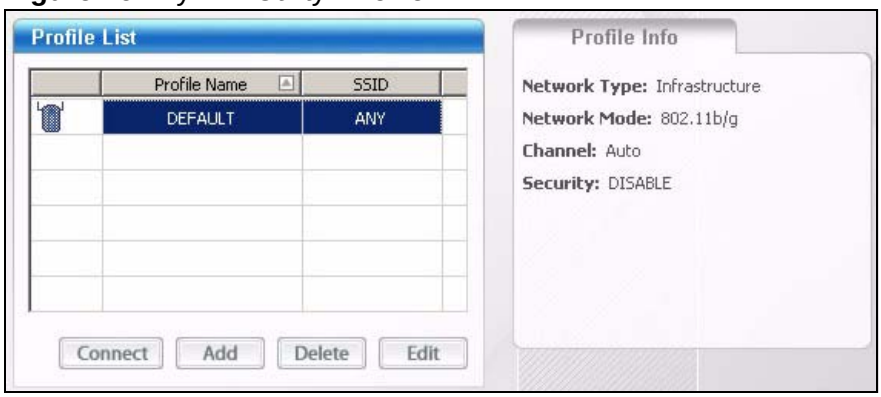
2.2.3.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the wireless client. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the SSID is “SSID_Example3”, the profile name is “PN_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”. You have chosen the profile name “PN_Example3”.

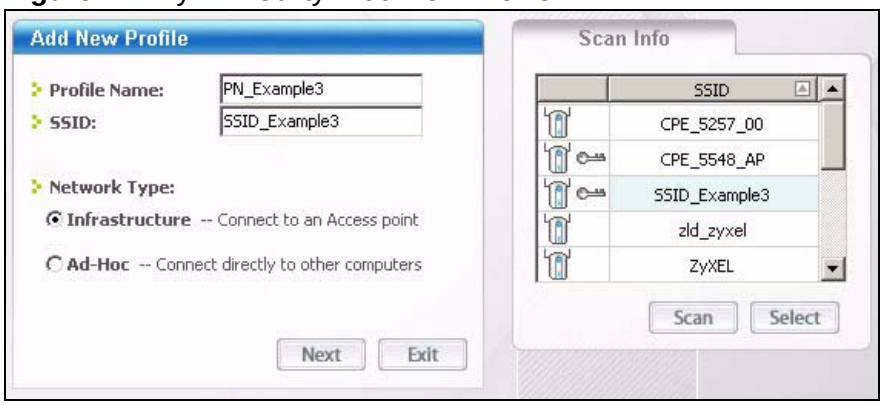
1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

Figure 16 ZyXEL Utility: Profile



2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. Click on **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.

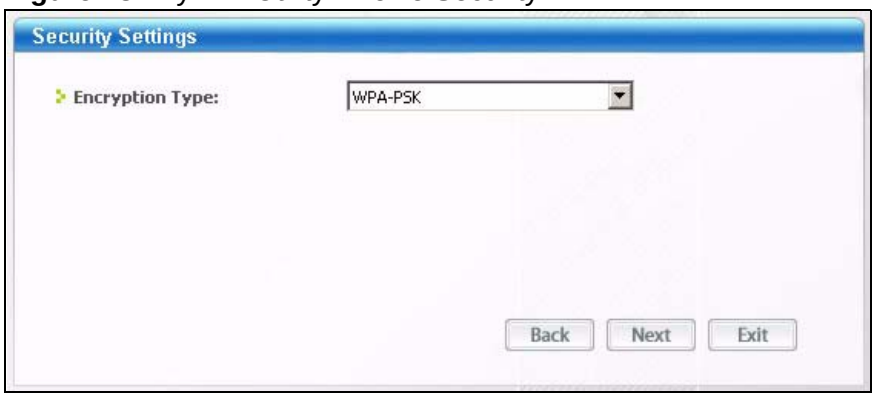
Figure 17 ZyXEL Utility: Add New Profile



3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

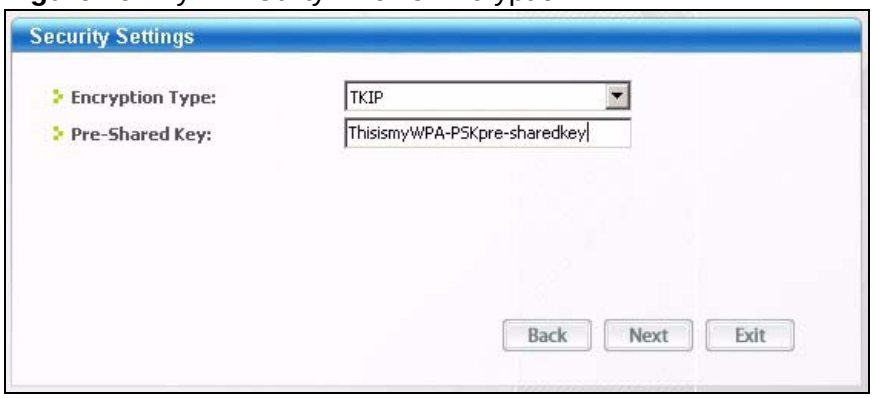
4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

Figure 18 ZyXEL Utility: Profile Security



5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.

Figure 19 ZyXEL Utility: Profile Encryption

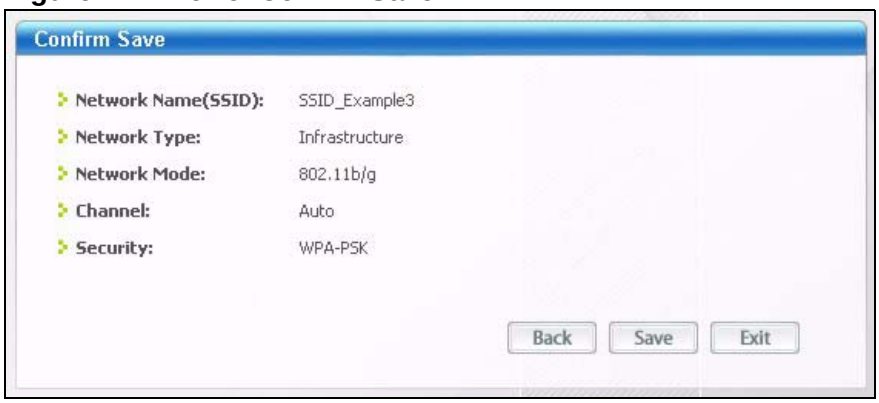


6 In the next screen, leave both boxes checked.

Figure 20 Profile: Wireless Protocol Settings.

7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.

Figure 21 Profile: Confirm Save



8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.

Figure 22 Profile: Activate

9 When you activate the new profile, the ZyXEL utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.

10 Open your Internet browser, enter http://www.zyxel.com or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.

11 If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

2.3 How to Use ATM QoS with Multiple PVCs and Interface Groups

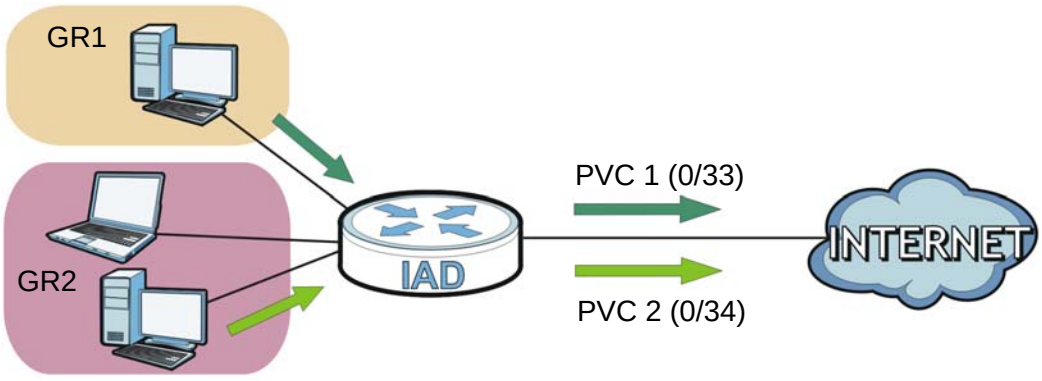
Note: Voice traffic will not be affected by the user-defined QoS settings on the P-2812HNU-51c. It always gets the highest priority.

The P-2812HNU-51c allows you to have more than one PVC using the ATM layer-2 interface. You can apply different ATM QoS settings to traffic through different PVCs. In this example, real-time or video service, such as using a webcam to send photos or uploading media content to share videos and images on a blog, comes from LAN 1 and is forwarded out through PVC 1 (0/33). Non-time sensitive data transfers, such as e-mail or FTP, come from LAN 2 or LAN 3 and are forwarded out through PVC 2 (0/34). The maximum upstream transmission speed of your ADSL port is 1 Mbps. You want to give the real-time traffic fixed bandwidth 400 Kbps and higher priority over the general data transmission which shares the bandwidth 600 Kbps.

Table 2 ATM QoS and Group Settings

TRAFFIC TYPE	LAN	PVC	ATM QOS	BANDWIDTH	GROUP
Real-time or video service	LAN1	atm1 (0/33)	CBR	400 Kbps	GR1
Non-time sensitive data	LAN2, LAN3	atm2 (0/34)	Non Realtime VBR	600 Kbps	GR2

Note: To apply different QoS priorities to different applications over a PVC, use the **Advanced > QoS** screens. The packet-level QoS feature is not applicable to a PVC with CBR or Realtime VBR enabled.



Overview of what you have to do

1 Create PVCs using the **Network > WAN** screens. See Figure 2.3.1 on page 44.

2 Create interface groups in the **Advanced Setup > Interface Group** screen to map logical LAN groups to the PVCs you created. See Figure 2.3.2 on page 53.

3 Configure IP addresses for devices in each interface group using the **Network > LAN** screen. See Figure 2.3.3 on page 57.

2.3.1 Configuring PVCs

Follows the steps below to set up two PVCs on the P-2812HNU-51c.

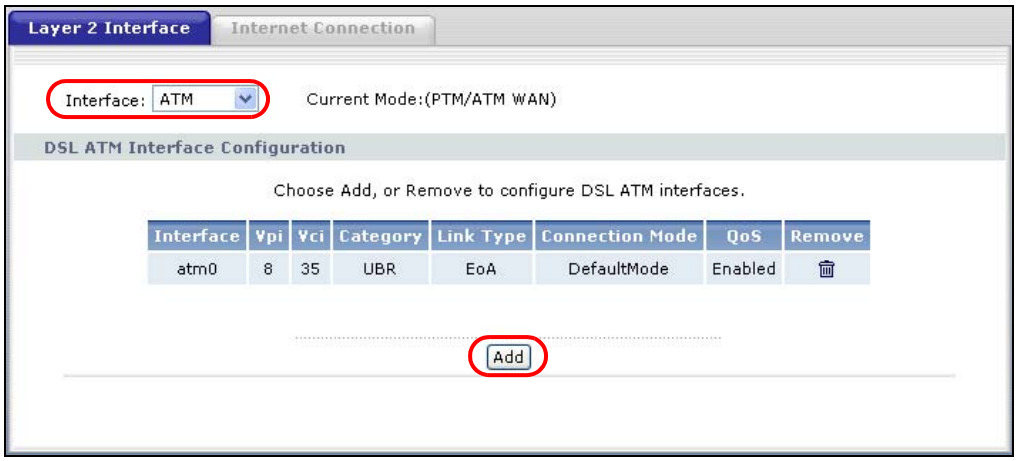
Table 3 Multiple PVC Settings

PVC	LAYER-2 INTERFACE	WAN SERVICE
0/33	atm1	PPPoE (pppoe_0_0_33)
0/34	atm2	IPoE (ipoe_0_0_34)

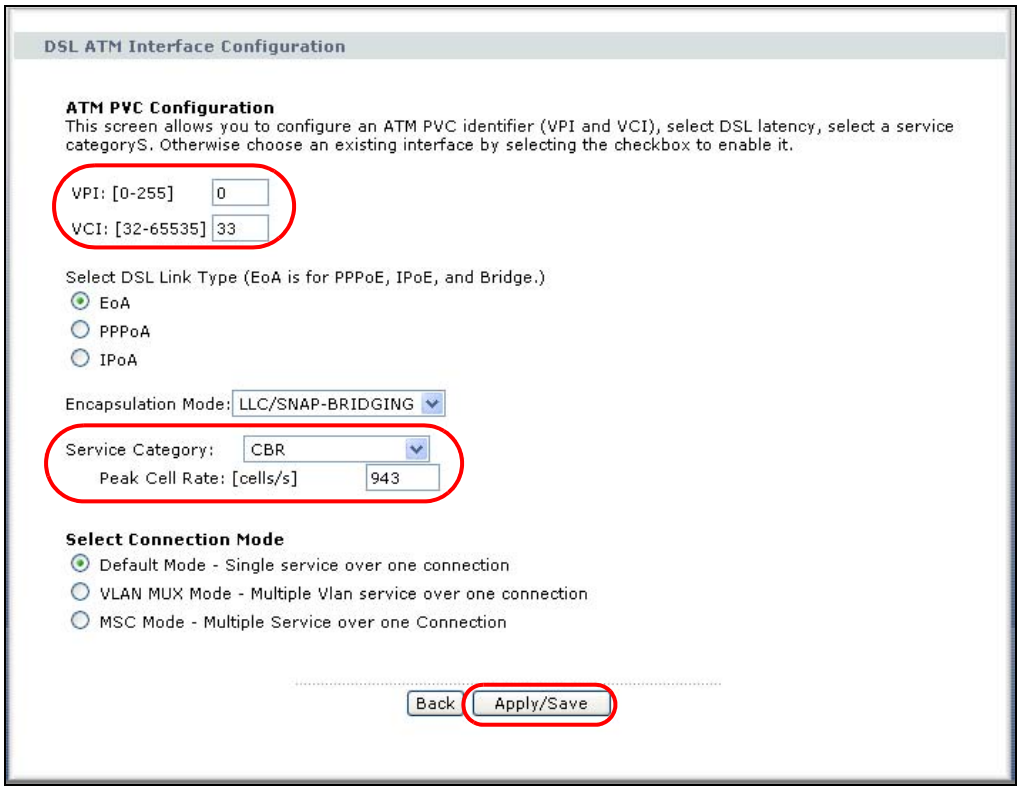
Note: Make sure you set the **DSL/WAN** switch (on the back of the P-2812HNU-51c) to the **DSL** side.

1 Click **Network > WAN** > **Layer 2 Interface**.

2 Select **ATM** from the **Interface** drop-down list and click **Add**.



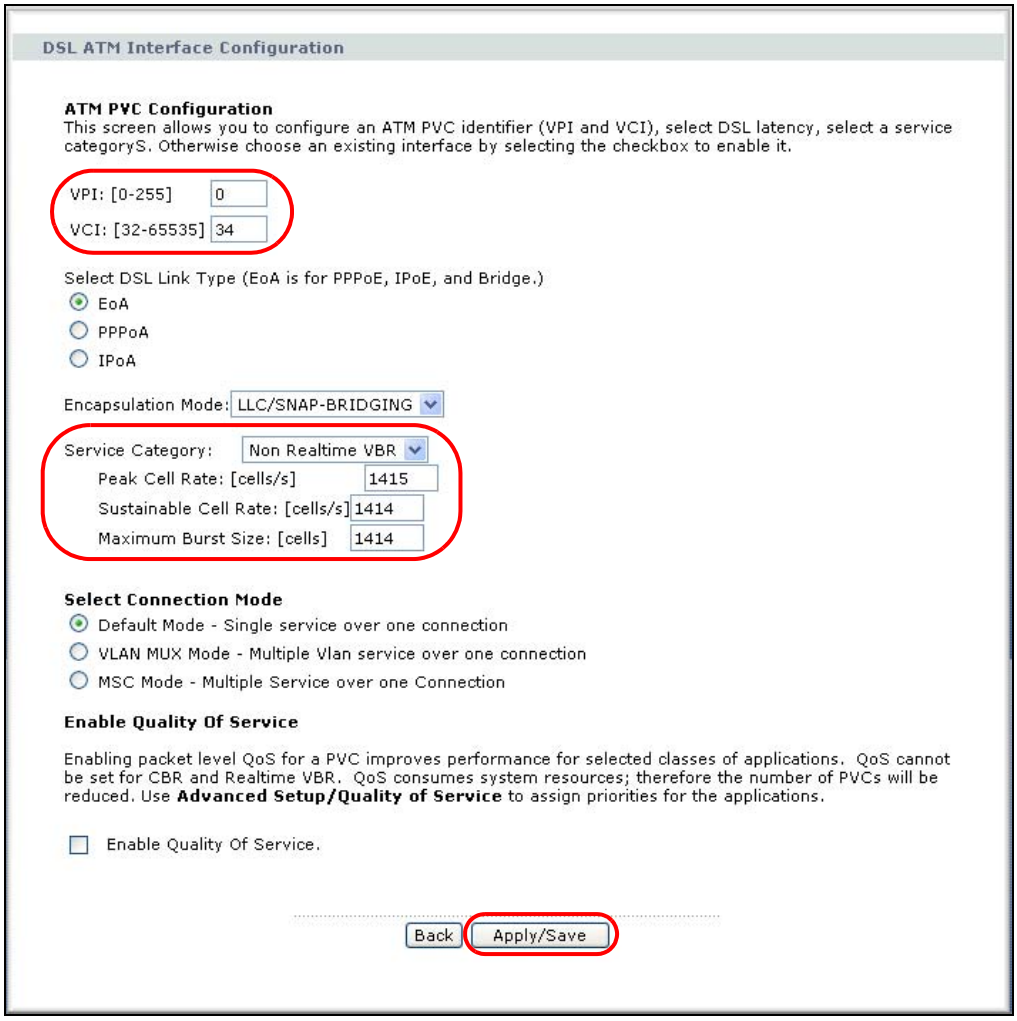
3 Enter the VPI and VCI values (**0** and **33** in this example) for PVC 1. Select **CBR** in the **Service Category** field and set the **Peak Cell Rate** as **943** (divide the bandwidth 400000 bps by 424). Click **Apply/Save** to save the changes and go back to the **Layer 2 Interface** screen.


DSL ATM Interface Configuration
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 0
VCI: [32-65535] 33
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
EoA
PPPoA
IPoA
Encapsulation Mode: LLC/SNAP-BRIDGING
Service Category: CBR
Peak Cell Rate: [cells/s] 943
Select Connection Mode
Default Mode - Single service over one connection
VLAN MUX Mode - Multiple Vlan service over one connection
MSC Mode - Multiple Service over one Connection
Back
Apply/Save

4 Click **Add** to configure another PVC.

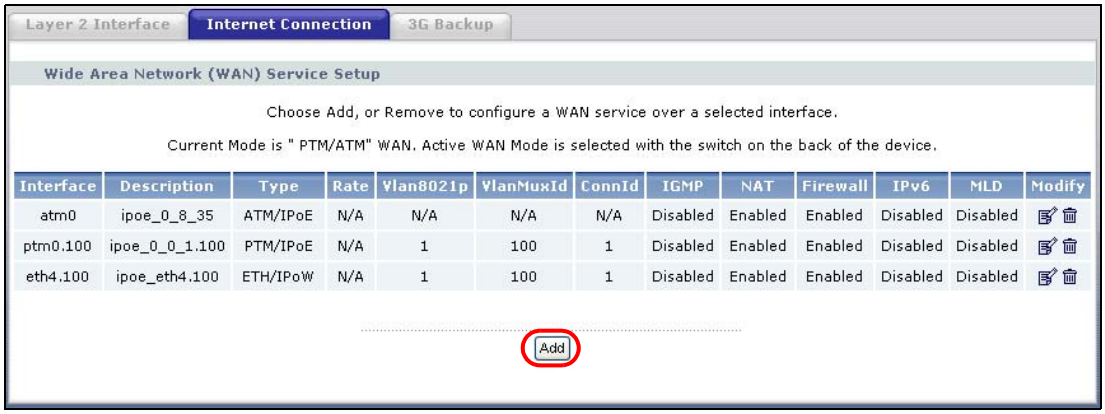
5 Enter the VPI and VCI values (**0** and **34** in this example) for PVC 2. Select **Non Realtime VBR** in the **Service Category** field. Set the **Peak Cell Rate** as **1415** (divide the bandwidth 600000 bps by 424) and set both the **Sustainable Cell Rate** and **Maximum Burst Size** as **1414** (which is less than the peak cell rate).

6 Click **Apply/Save** to save the changes and go back to the **Layer 2 Interface** screen.

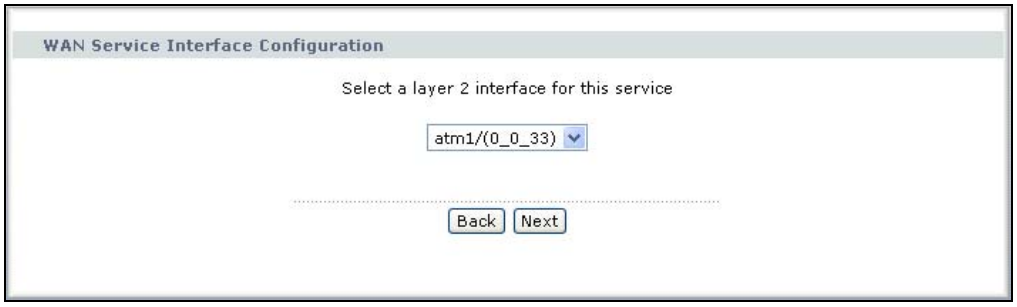

DSL ATM Interface Configuration
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 0
VCI: [32-65535] 34
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
EoA
PPPoA
IPoA
Encapsulation Mode: LLC/SNAP-BRIDGING
Service Category: Non Realtime VBR
Peak Cell Rate: [cells/s] 1415
Sustainable Cell Rate: [cells/s] 1414
Maximum Burst Size: [cells] 1414
Select Connection Mode
Default Mode - Single service over one connection
VLAN MUX Mode - Multiple Vlan service over one connection
MSC Mode - Multiple Service over one Connection
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service.
Back
Apply/Save

2.3.1.1 Internet Connection Settings for PVC 1

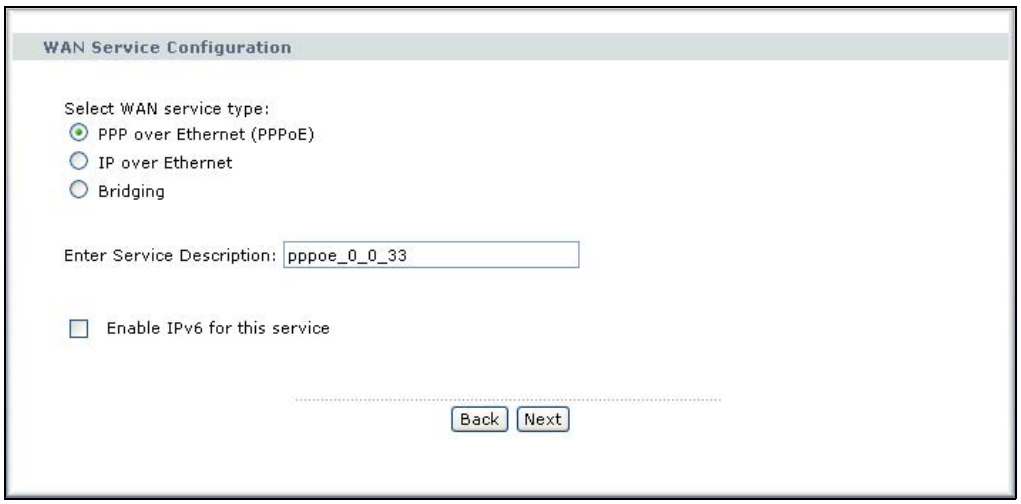
1 Click **Network > WAN** > **Internet Connection** to configure WAN connection settings for PVC 1. Click **Add**.


Layer 2 Interface
Internet Connection
3G Backup
Wide Area Network (WAN) Service Setup
Choose Add, or Remove to configure a WAN service over a selected interface.
Current Mode is " PTM/ATM" WAN. Active WAN Mode is selected with the switch on the back of the device.
Interface Description Type Rate Vlan8021p VlanMuxId ConnId IGMP NAT Firewall IPv6 MLD Modify
atm0 ipoe_0_8_35 ATM/IPoE N/A N/A N/A N/A Disabled Enabled Enabled Disabled Disabled
ptm0.100 ipoe_0_0_1.100 PTM/IPoE N/A 1 100 1 Disabled Enabled Enabled Disabled Disabled
eth4.100 ipoe_eth4.100 ETH/IPoW N/A 1 100 1 Disabled Enabled Enabled Disabled Disabled
Add

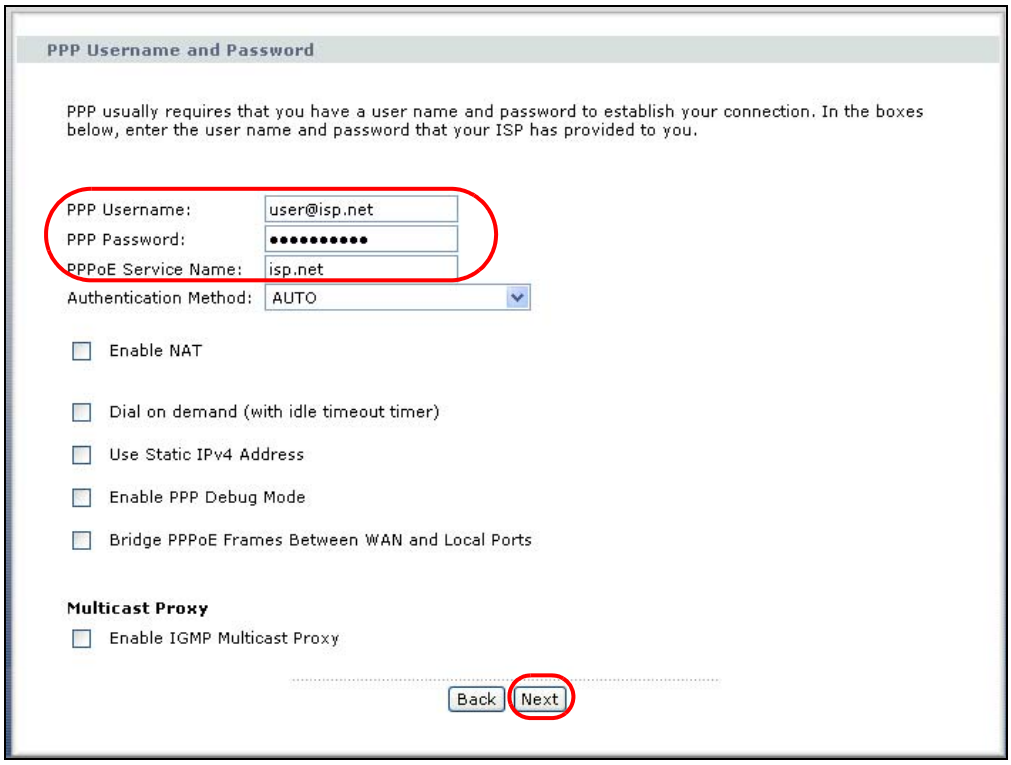
2 Select PVC 1 (**atm1/0_0_33**) as the layer-2 interface. Click **Next**.



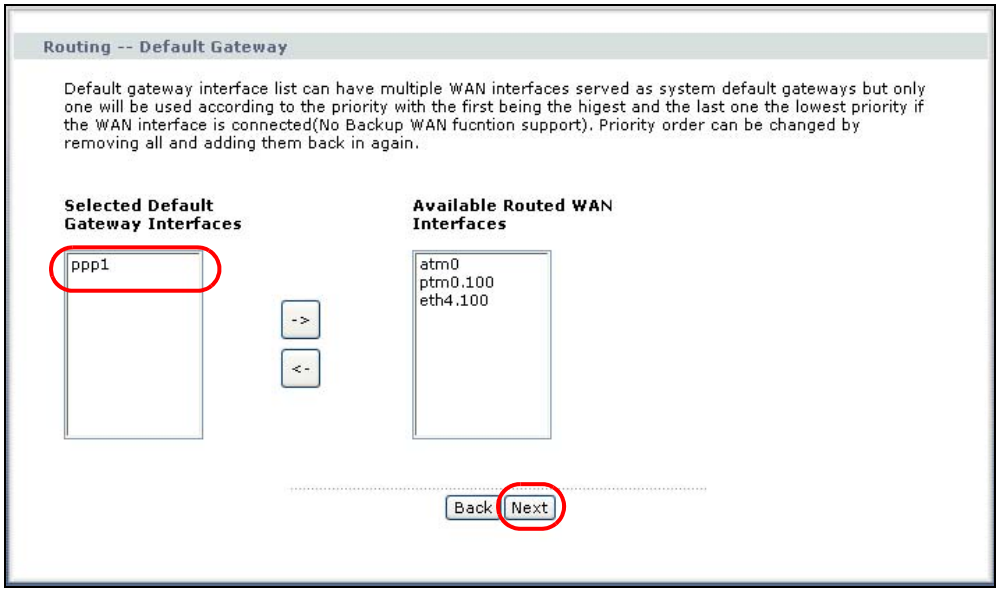
3 Select **PPP over Ethernet** and click **Next**.



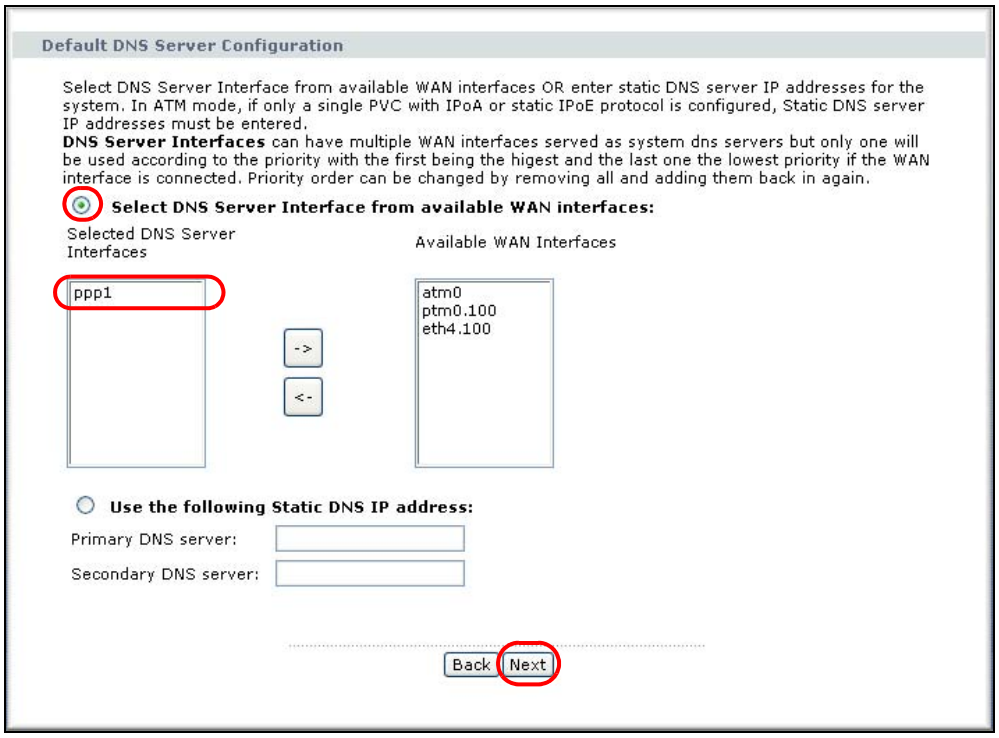
4 Enter the user name (**user@isp.net** for example), password (**qwert12345** for example) and service name (**isp.net** for example) for the PPP connection. Click **Next**.


PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
user@isp.net
PPP Password:
PPPoE Service Name:
isp.net
Authentication Method:
AUTO
Enable NAT
Dial on demand (with idle timeout timer)
Use Static IPv4 Address
Enable PPP Debug Mode
Bridge PPPoE Frames Between WAN and Local Ports
Multicast Proxy
Enable IGMP Multicast Proxy
Back
Next

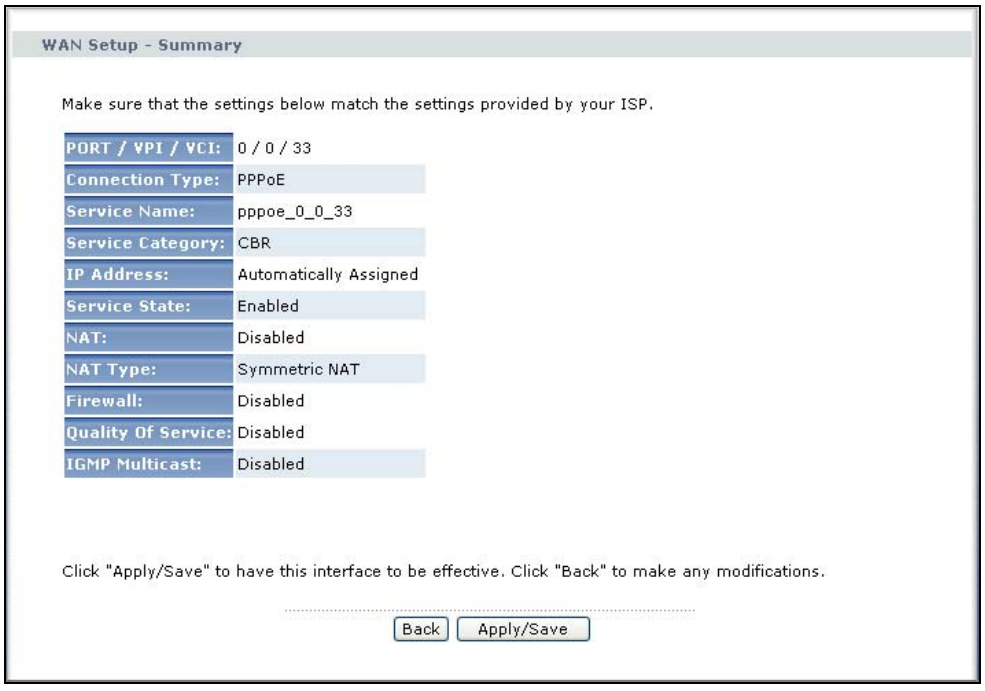
5 Remove the existing interfaces in the **Selected Default Gateway Interfaces** list. Select and move a WAN interface (**ppp1** in this example) to the **Selected Default Gateway Interfaces** list to use that interface as the default gateway. Click **Next**.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected(No Backup WAN fucntion support). Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
ppp1
->
<-
Available Routed WAN Interfaces
atm0
ptm0.100
eth4.100
Back
Next

6 Select the first option. Remove the existing interfaces in the **Selected DNS Server Interfaces** list. Select and move a WAN interface (**ppp1** in this example) to the **Selected DNS Server Interfaces** list to use that interface as the system DNS server. Click **Next**.


Default DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
ppp1
atm0
ptm0.100
eth4.100
->
<-
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Back
Next

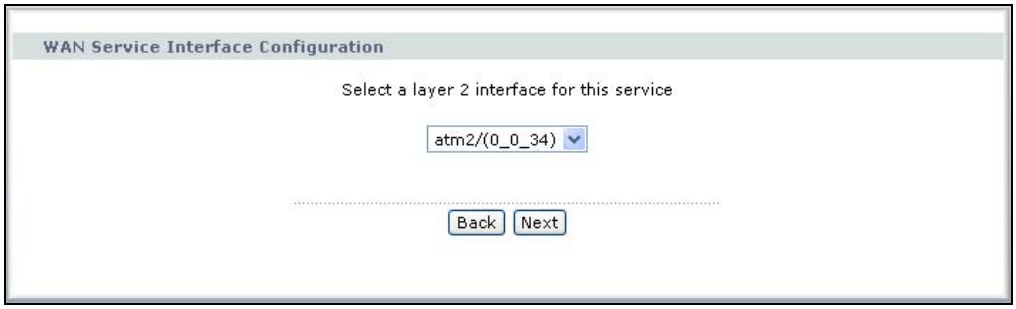
7 The summary screen displays. Click **Apply/Save** to save your changes and go back to the **Internet Connection** screen.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
PORT / VPI / VCI: 0 / 0 / 33
Connection Type: PPPoE
Service Name: pppoe_0_0_33
Service Category: CBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Disabled
NAT Type: Symmetric NAT
Firewall: Disabled
Quality Of Service: Disabled
IGMP Multicast: Disabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

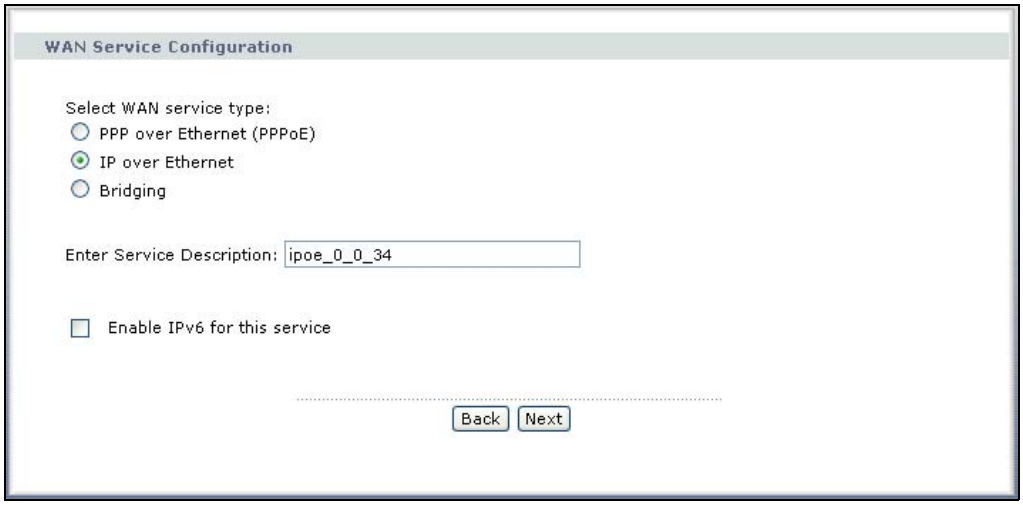
2.3.1.2 Internet Connection Settings for PVC 2

1 Click **Add** in the **WAN > Internet Connection** screen to configure WAN connection settings for PVC 2.

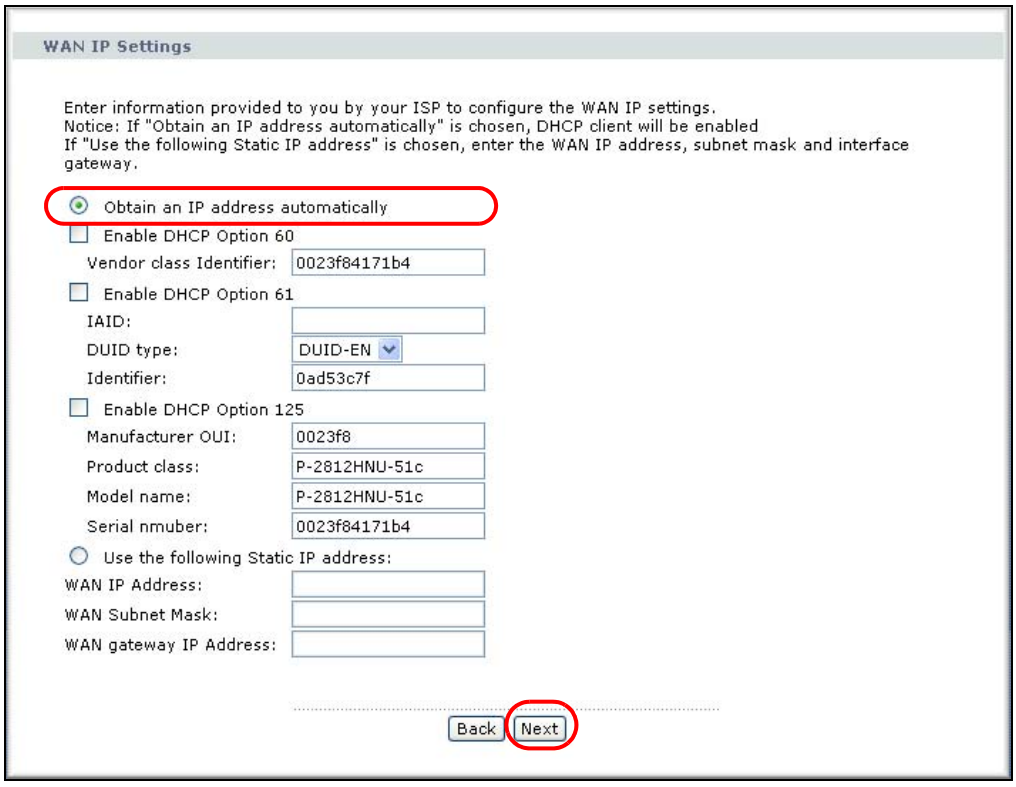
2 Select PVC 2 (**atm2/0_0_34**) as the layer-2 interface. Click **Next**.



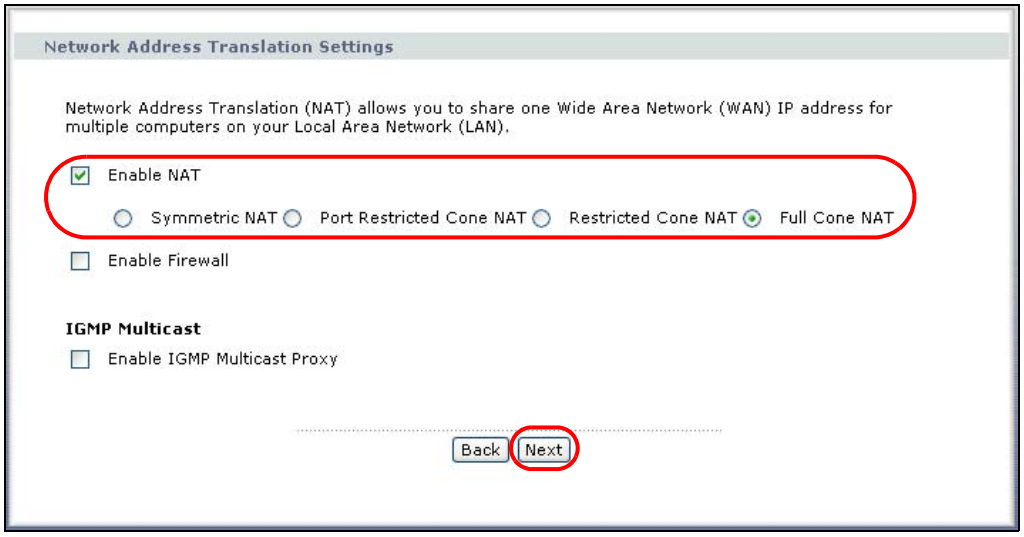
3 Select **IP over Ethernet** and click **Next**.



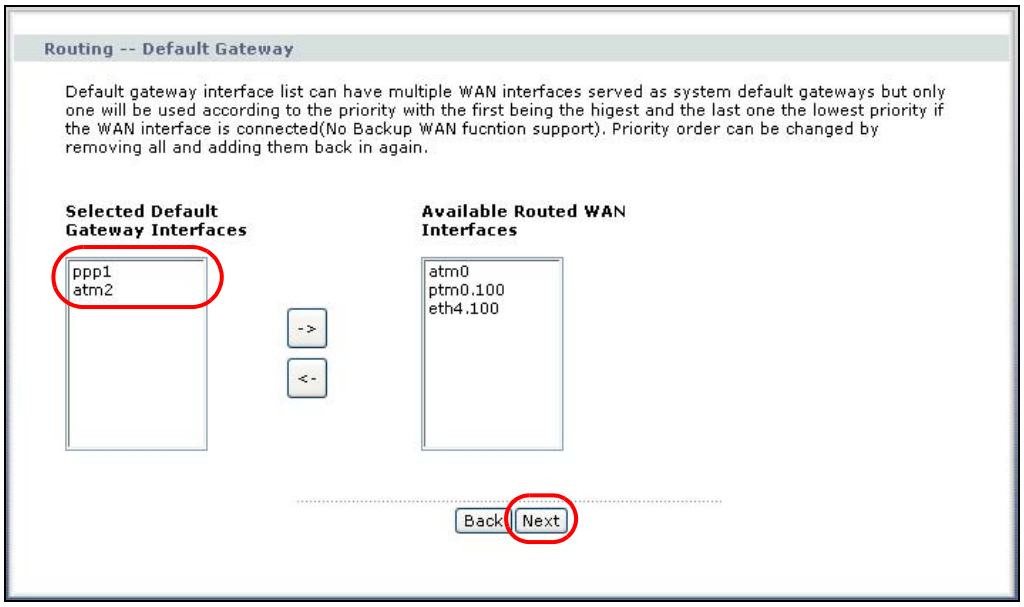
4 Select **Obtain an IP address automatically** and click **Next**.


WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP client will be enabled
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.
Obtain an IP address automatically
Enable DHCP Option 60
Vendor class Identifier: 0023f84171b4
Enable DHCP Option 61
IAID:
DUID type: DUID-EN
Identifier: 0ad53c7f
Enable DHCP Option 125
Manufacturer OUI: 0023f8
Product class: P-2812HNU-51c
Model name: P-2812HNU-51c
Serial nmuber: 0023f84171b4
Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:
Back
Next

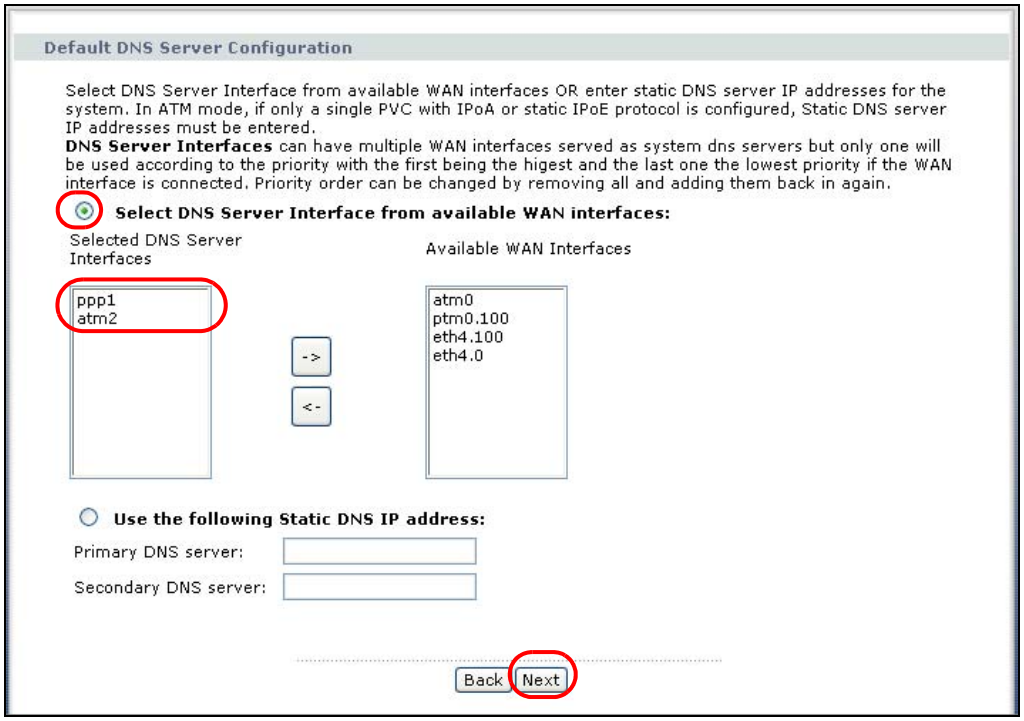
5 Select **Enable NAT** and **Full Cone NAT**, then click **Next**.


Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Symmetric NAT
Port Restricted Cone NAT
Restricted Cone NAT
Full Cone NAT
Enable Firewall
IGMP Multicast
Enable IGMP Multicast Proxy
Back
Next

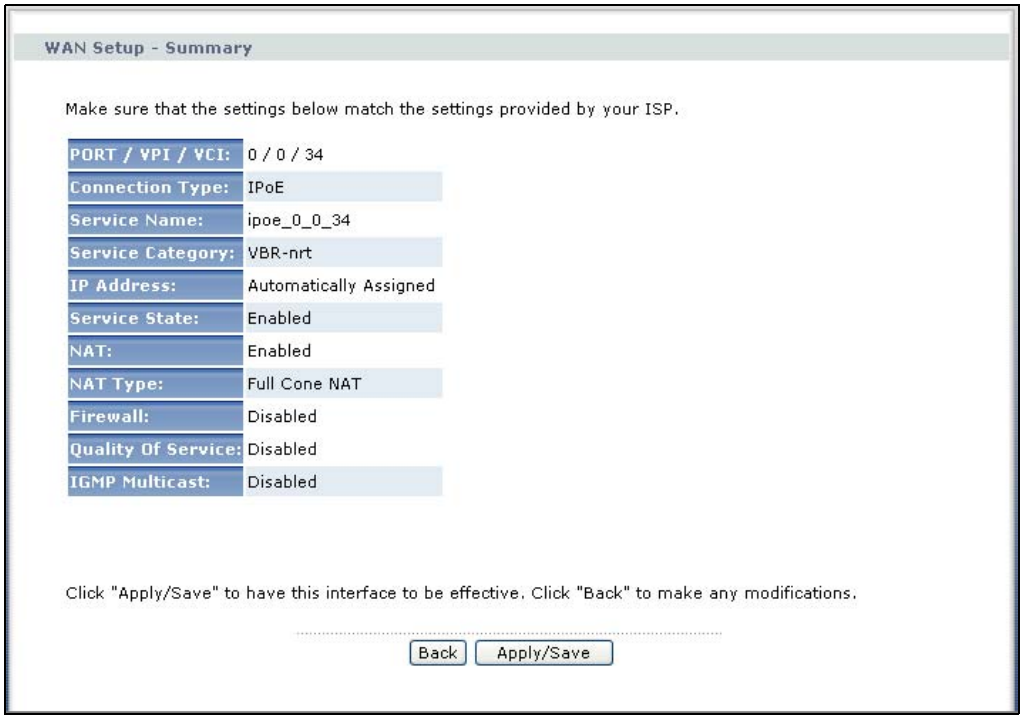
6 Select and move the WAN interface (**atm2** in this example) to the **Selected Default Gateway Interfaces** list to use that interface as the default gateway. Click **Next**.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected(No Backup WAN fucntion support). Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ppp1
atm2
atm0
ptm0.100
eth4.100
->
<-
Back
Next

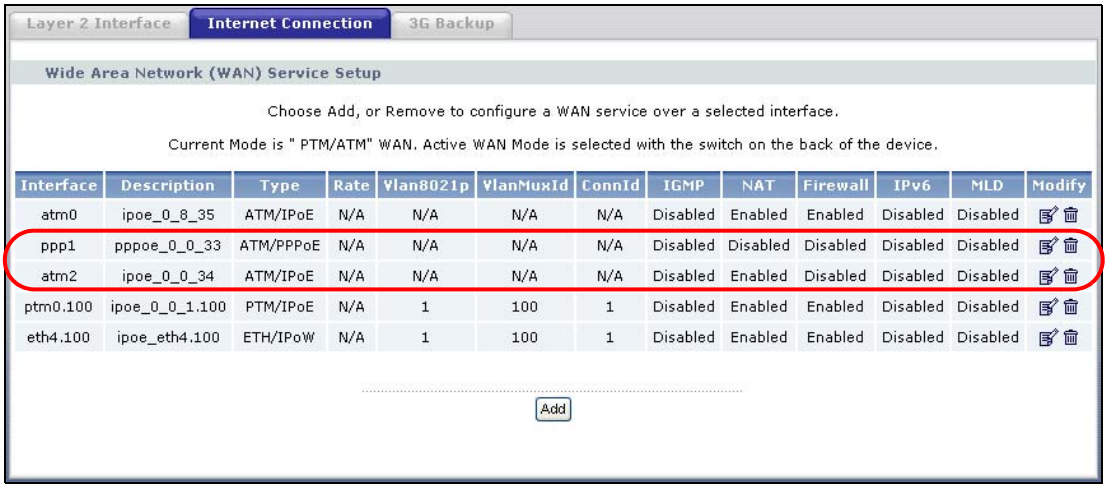
7 Select the first option. Select and move the WAN interface (**atm2** in this example) to the **Selected DNS Server Interfaces** list to use that interface as the system DNS server. Click **Next**.


Default DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
ppp1
atm2
atm0
ptm0.100
eth4.100
eth4.0
->
<-
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Back
Next

8 The summary screen displays. Click **Apply/Save** to save your changes and go back to the **Internet Connection** screen.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
PORT / VPI / VCI: 0 / 0 / 34
Connection Type: IPoE
Service Name: ipoe_0_0_34
Service Category: VBR-nrt
IP Address: Automatically Assigned
Service State: Enabled
NAT: Enabled
NAT Type: Full Cone NAT
Firewall: Disabled
Quality Of Service: Disabled
IGMP Multicast: Disabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

9 The **Internet Connection** screen should look like the following.


Layer 2 Interface
Internet Connection
3G Backup
Wide Area Network (WAN) Service Setup
Choose Add, or Remove to configure a WAN service over a selected interface.
Current Mode is " PTM/ATM" WAN. Active WAN Mode is selected with the switch on the back of the device.
Interface Description Type Rate Vlan8021p VlanMuxId ConnId IGMP NAT Firewall IPv6 MLD Modify
atm0 ipoe_0_8_35 ATM/IPoE N/A N/A N/A N/A Disabled Enabled Enabled Disabled Disabled
ppp1 pppoe_0_0_33 ATM/PPPoE N/A N/A N/A N/A Disabled Disabled Disabled Disabled Disabled
atm2 ipoe_0_0_34 ATM/IPoE N/A N/A N/A N/A Disabled Enabled Disabled Disabled Disabled
ptm0.100 ipoe_0_0_1.100 PTM/IPoE N/A 1 100 1 Disabled Enabled Enabled Disabled Disabled
eth4.100 ipoe_eth4.100 ETH/IPoW N/A 1 100 1 Disabled Enabled Enabled Disabled Disabled
Add

2.3.2 Setting Interface Groups

This part shows examples of creating multiple networks groups with the WAN services that you have configured in the previous section.

Follow the steps below to map traffic from LAN 1 to PVC 1 and traffic from LAN 2 and LAN 3 to PVC 2.

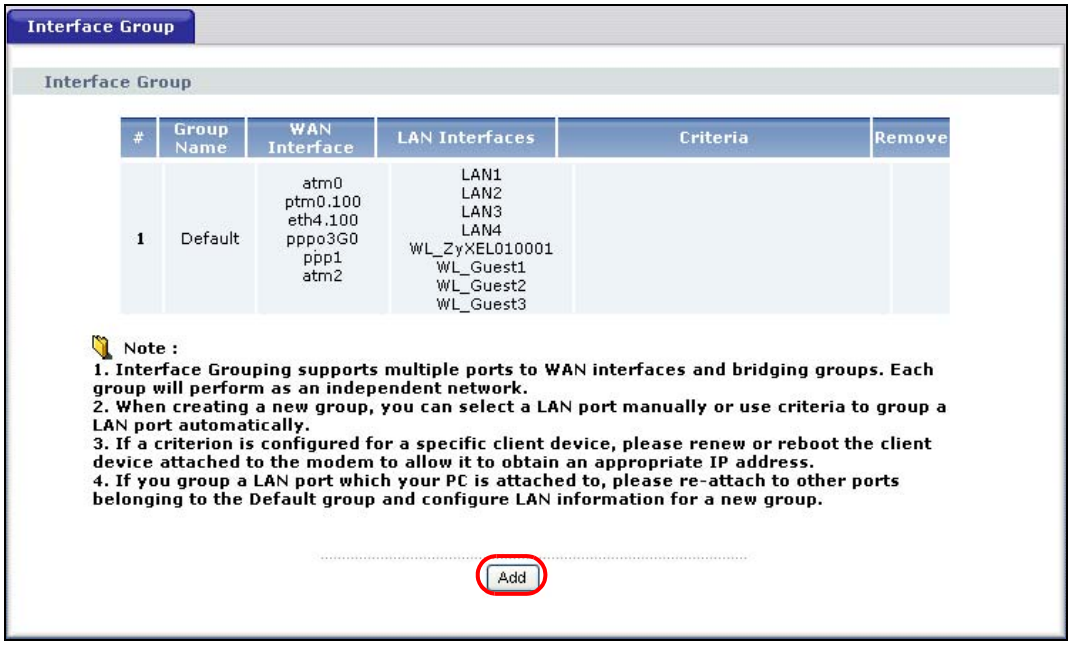
Table 4 DSL Connection Groups

GROUP	LAN IP ADDRESS	LAN INTERFACE	WAN INTERFACE
GR1	192.168.2.x	LAN1	ppp1 (0/33)
GR2	192.168.3.x	LAN2, LAN3	atm2 (0/34)

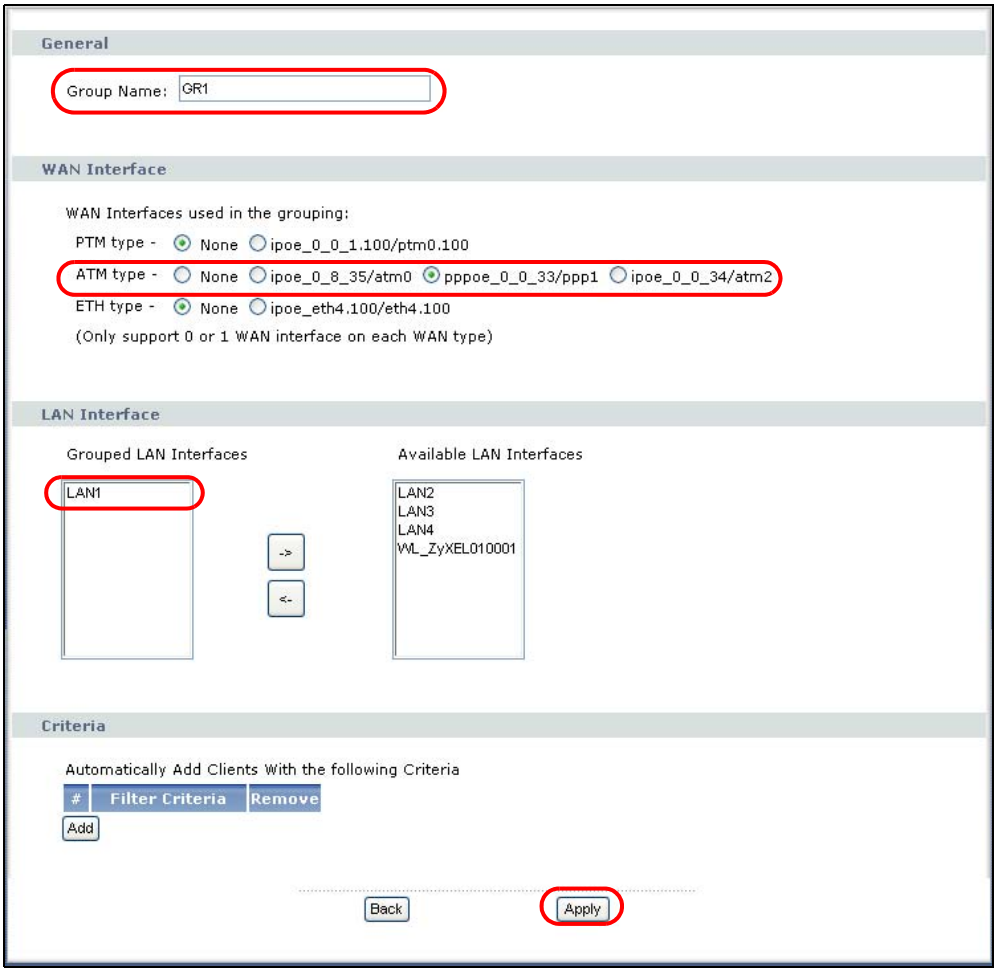
Note: Before configuring interface groups, make sure you are connected to LAN 4 which will not be in a group other than the default group. Otherwise, you need to use the IP address of the new group to access the P-2812HNU-51c after you apply the changes.

Note: You can also use policy forwarding to map traffic from a LAN port to a specific PVC, but you need to enter the source IP address, port number and/or MAC address of each packet that comes from the LAN port. See Chapter 16 on page 297 for more information.

1 Click **Advanced Setup > Interface Group** to open the following screen. Click **Add** to create a new interface group **GR1**.

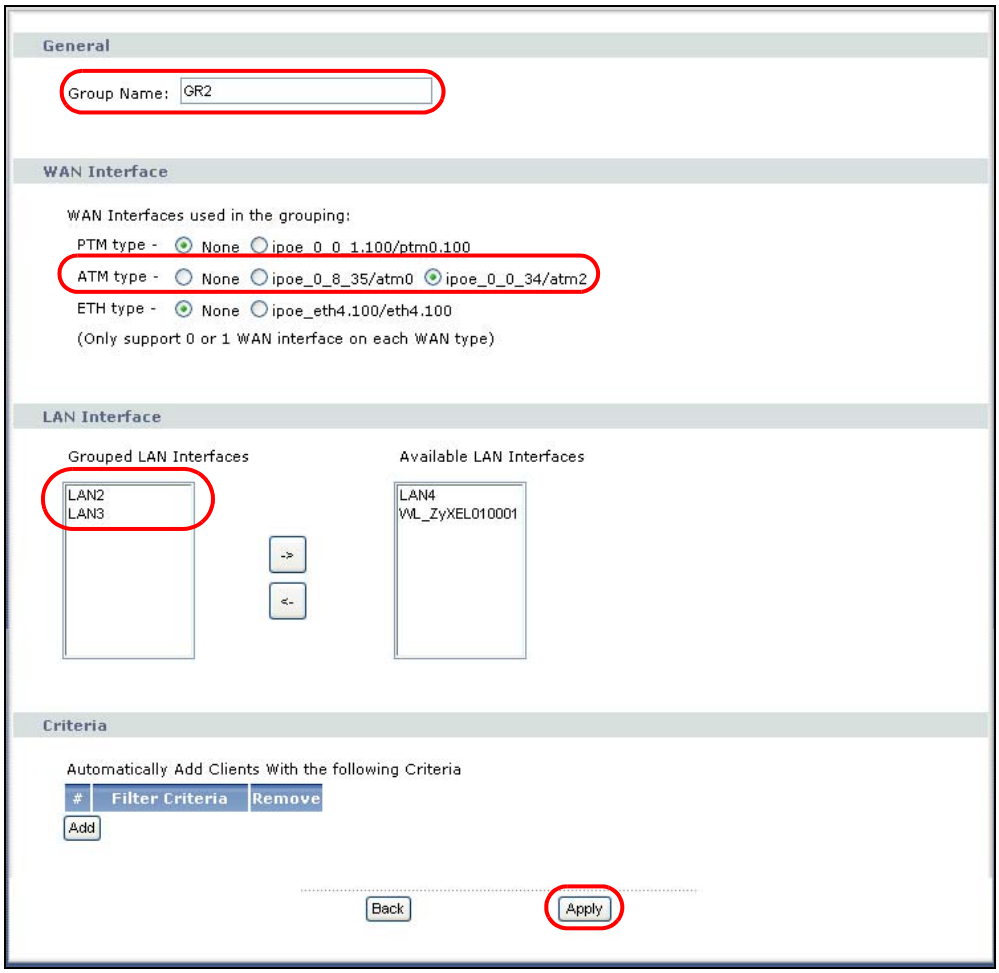

Interface Group
Interface Group
Group Name WAN Interface LAN Interfaces Criteria Remove
1 Default atm0 ptm0.100 eth4.100 pppo3G0 ppp1 atm2 LAN1 LAN2 LAN3 LAN4 WL_ZyXEL010001 WL_Guest1 WL_Guest2 WL_Guest3
Note :
1. Interface Grouping supports multiple ports to WAN interfaces and bridging groups. Each group will perform as an independent network.
2. When creating a new group, you can select a LAN port manually or use criteria to group a LAN port automatically.
3. If a criterion is configured for a specific client device, please renew or reboot the client device attached to the modem to allow it to obtain an appropriate IP address.
4. If you group a LAN port which your PC is attached to, please re-attach to other ports belonging to the Default group and configure LAN information for a new group.
Add

2 Enter **GR1** as the **Group Name**. In this group, we will associate **ppp1** (PVC 1) as the WAN interface with LAN1 as the LAN interface. Select **pppoe_0_0_33/ppp1** from the **WAN Interface** list. Select **LAN1** from the **Available LAN Interfaces** list and click <- to add it to the **Grouped LAN Interfaces**. Click **Apply** to finish the settings and go back to the **Interface Group** screen.

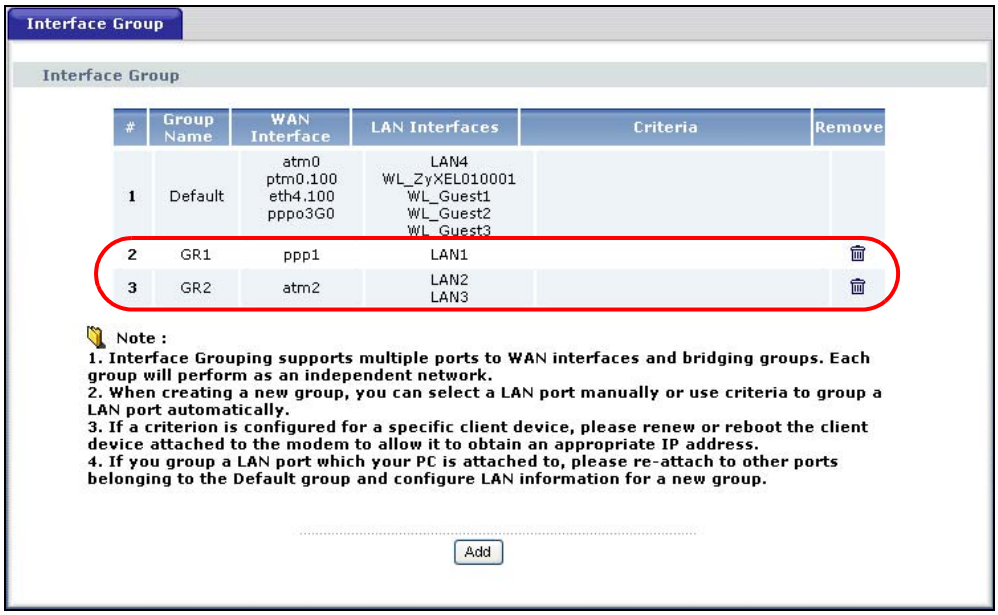


3 **GR1** has been added successfully to the interface group list. Click **Add** to create another interface group: **GR2**.

4 Enter **GR2** as the **Group Name**. In this group, we will associate **atm2** (PVC 2) as the WAN interface with LAN2 and LAN3 as the LAN interfaces. Select **ipoe_0_0_34/atm2** from the **WAN Interface** list. Select **LAN2** and **LAN3** from the **Available LAN Interfaces** list and click <- to add them to the **Grouped LAN Interfaces**. Click **Apply** to finish the settings and go back to the **Interface Group** screen.



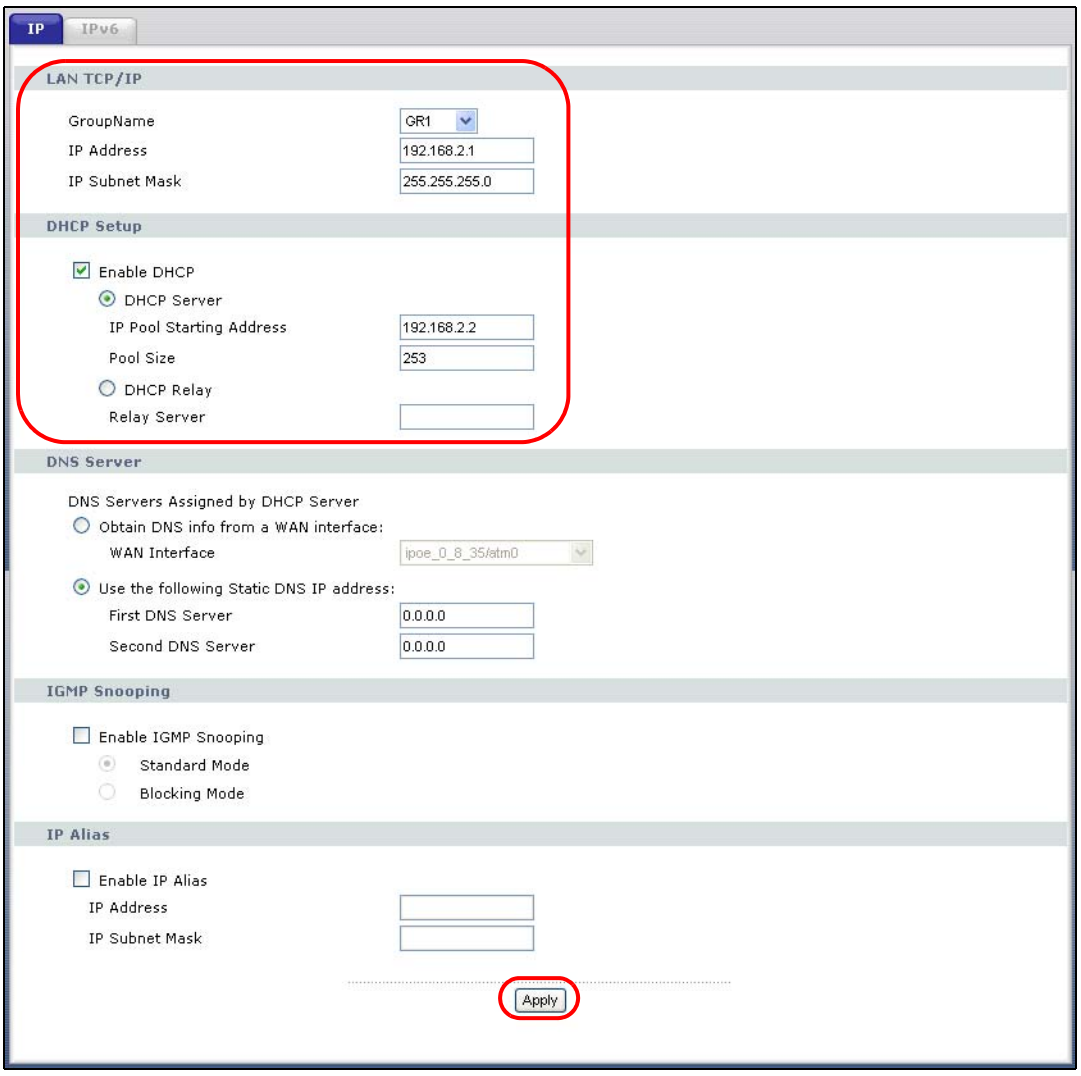
5 **GR2** has been added successfully to the interface group list. The screen should look like the following.


Interface Group
Interface Group
Group Name WAN Interface LAN Interfaces Criteria Remove
1 Default atm0 ptm0.100 eth4.100 pppo3G0 LAN4 WL_ZyXEL010001 WL_Guest1 WL_Guest2 WL_Guest3
2 GR1 ppp1 LAN1
3 GR2 atm2 LAN2 LAN3
Note :
1. Interface Grouping supports multiple ports to WAN interfaces and bridging groups. Each group will perform as an independent network.
2. When creating a new group, you can select a LAN port manually or use criteria to group a LAN port automatically.
3. If a criterion is configured for a specific client device, please renew or reboot the client device attached to the modem to allow it to obtain an appropriate IP address.
4. If you group a LAN port which your PC is attached to, please re-attach to other ports belonging to the Default group and configure LAN information for a new group.
Add

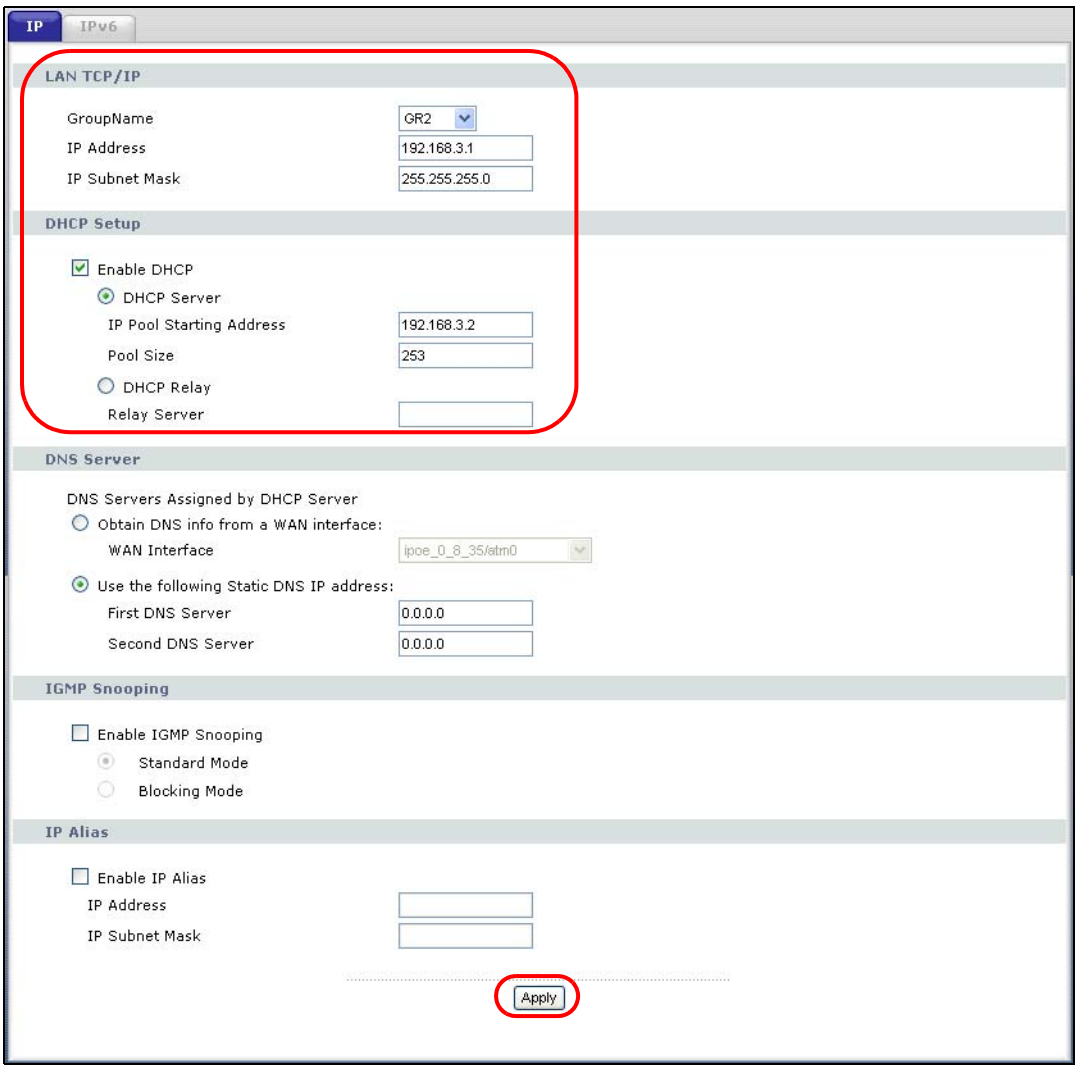
2.3.3 Configuring Interface Group IP

Follow the steps below to configure the P-2812HNU-51c's LAN IP address and DHCP settings for each group.

1 Click **Network** > **LAN**. Select **GR1** from the **GroupName** drop-down list. The **IP Address** (192.168.2.1) and **IP Subnet Mask** (255.255.255.0) are obtained automatically. Select **Active DHCP** and **DHCP Server** to have the ZyXEL Device act as the DHCP server for the network. Click **Apply** to save your changes.



2 Select **GR2** from the **GroupName** drop-down list. The **IP Address** (192.168.3.1) and **IP Subnet Mask** (255.255.255.0) are obtained automatically. Select **Active DHCP** and **DHCP Server** to have the ZyXEL Device act as the DHCP server for the network. Click **Apply** when you finish the settings.



2.3.4 Testing the DSL Connection Groups

To test if the connection groups are successfully configured, you can do the following: connect your computer to LAN1 of the P-2812HNU-51c. After a few seconds, the IP address of your computer should be renewed to 192.168.2.x automatically. If you can access Internet by using this DSL connection, GR1 is successfully configured.

To test GR2, connect your computer to LAN2 or LAN3 of the P-2812HNU-51c. After a few seconds, the IP address of your computer should be renewed to 192.168.3.x

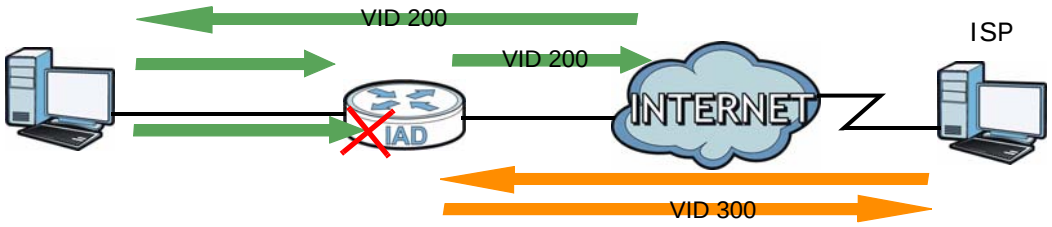
automatically. If you can access Internet by using this DSL connection, GR2 is successfully configured.

2.4 How to Allow Out-of-band Remote Management from the WAN

This tutorial shows you how to set up a dedicated WAN connection for ISP management of the P-2812HNU-51c and prevent the clients on the LAN from configuring the P-2812HNU-51c. You set up two DSL connections with different VLAN IDs and priorities to separate clients traffic from management traffic. The DSL connection for remote management has the highest priority.

Table 5 Multiple VDSL Connection Settings

WAN INTERFACE	DESCRIPTION	CONNECTION METHOD	VLAN ID	PRIORITY
ppp1.200	Internet	PPPoE	200	2
ptm0.300	RemoteMgmt	IPoE	300	7

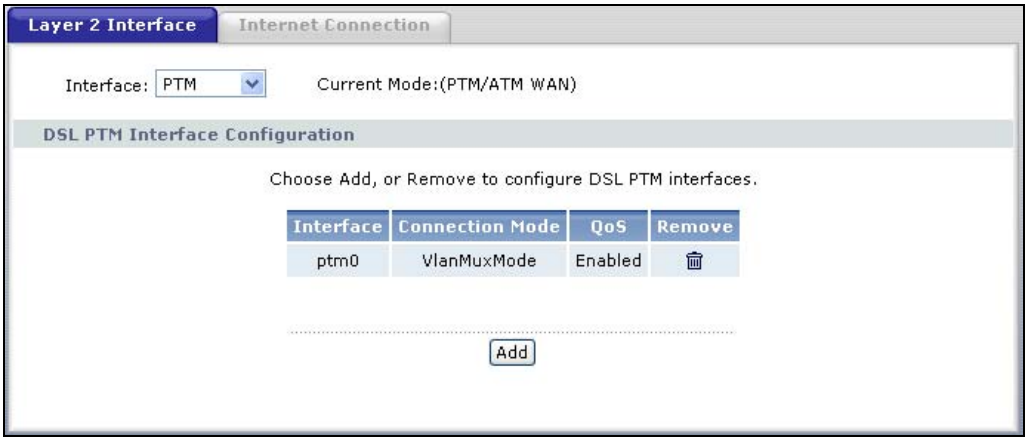


2.4.1 Configuring Multiple WAN Connections

Follow the steps below to configure two VDSL connections.

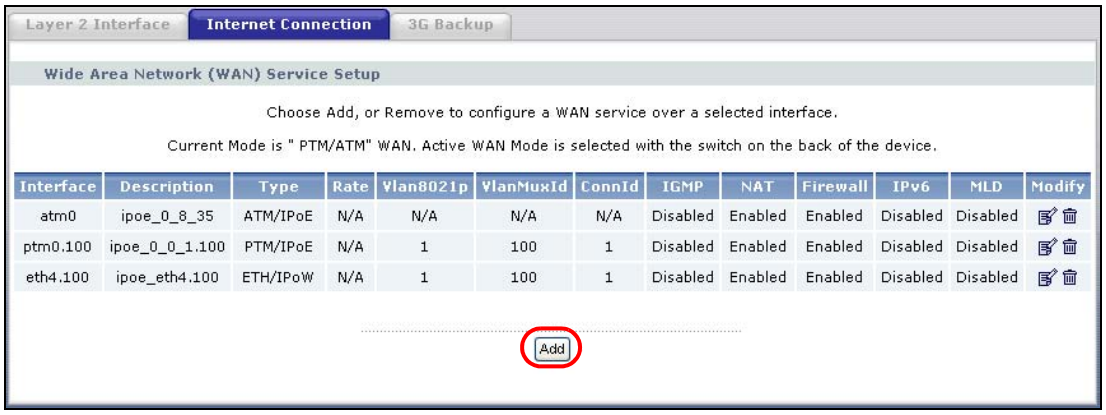
1 Make sure you set the **DSL / WAN** switch (on the back of the P-2812HNU-51c) to the **DSL** side.

2 By default, there is a PTM layer-2 interface in VLAN MUX mode configured already on the P-2812HNU-51c.

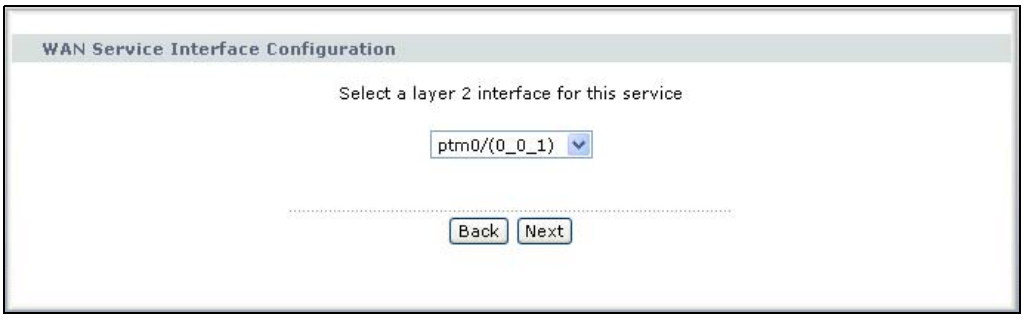


DSL Connection for Internet Access

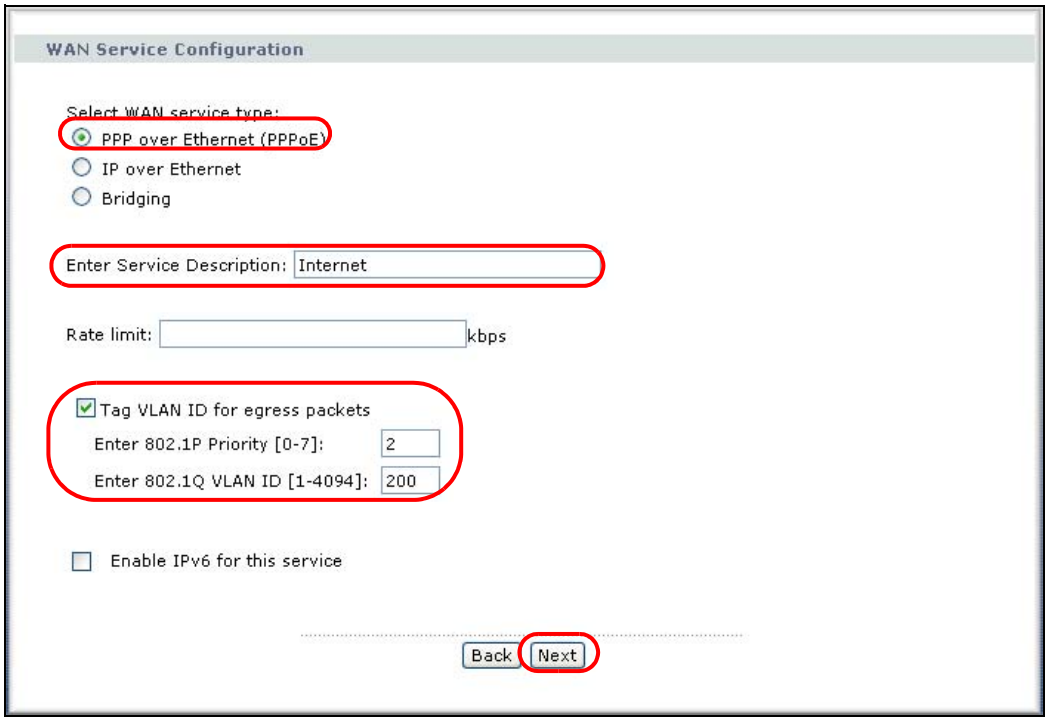
1 Go to the **WAN > Internet Connection** screen. Click **Add**.



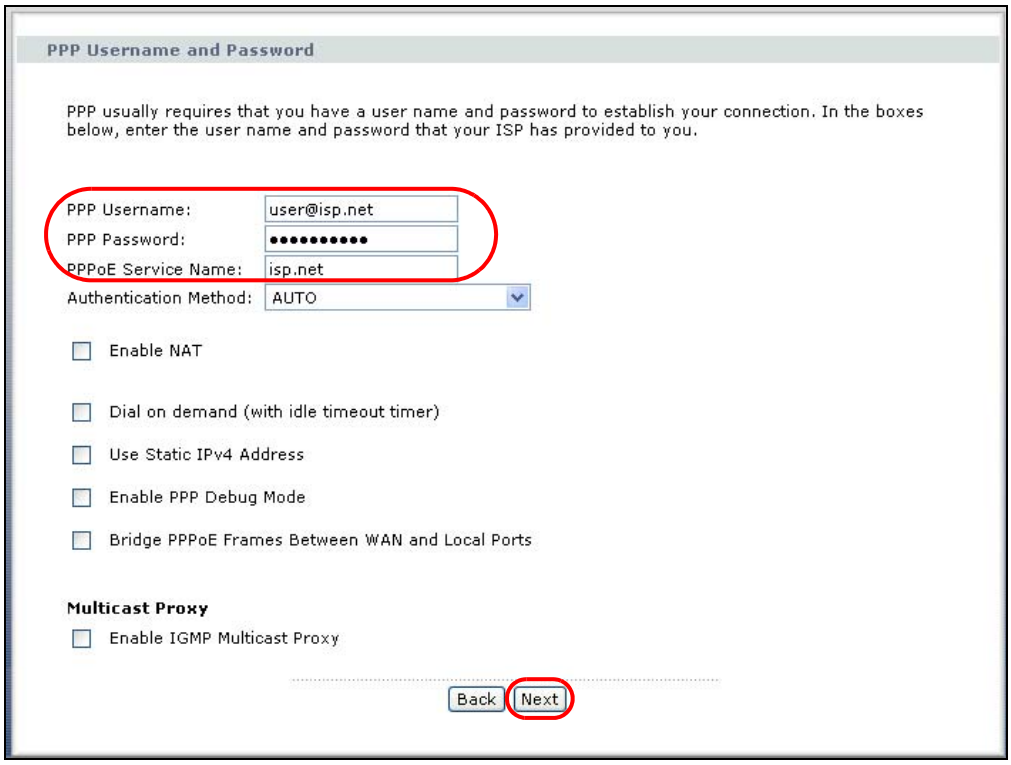
2 Select **ptm0/(0_0_1)** as the layer-2 interface. Click **Next**.



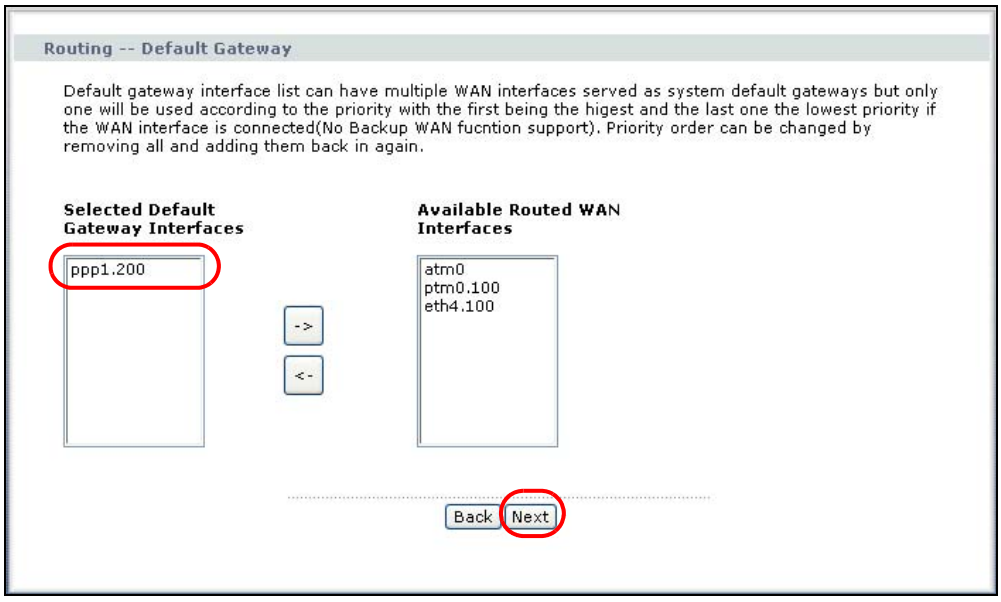
3 Select **PPP over Ethernet**, enter a descriptive service name (**Internet** in this example), and set the priority level to **2** and VLAN ID to **200**. Click **Next**.



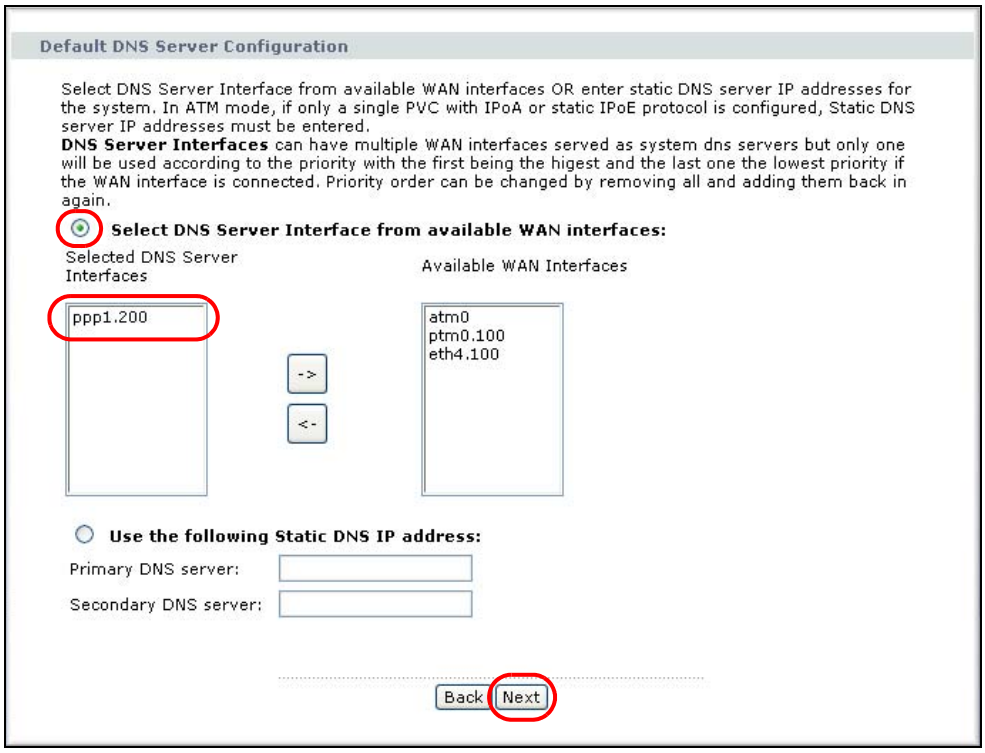
4 Enter the user name (**user@isp.net** for example), password (**qwert12345** for example) and service name (**isp.net** for example) for the PPP connection. Click **Next**.


PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username: user@isp.net
PPP Password: ••••••••••
PPPoE Service Name: isp.net
Authentication Method: AUTO
Enable NAT
Dial on demand (with idle timeout timer)
Use Static IPv4 Address
Enable PPP Debug Mode
Bridge PPPoE Frames Between WAN and Local Ports
Multicast Proxy
Enable IGMP Multicast Proxy
Back
Next

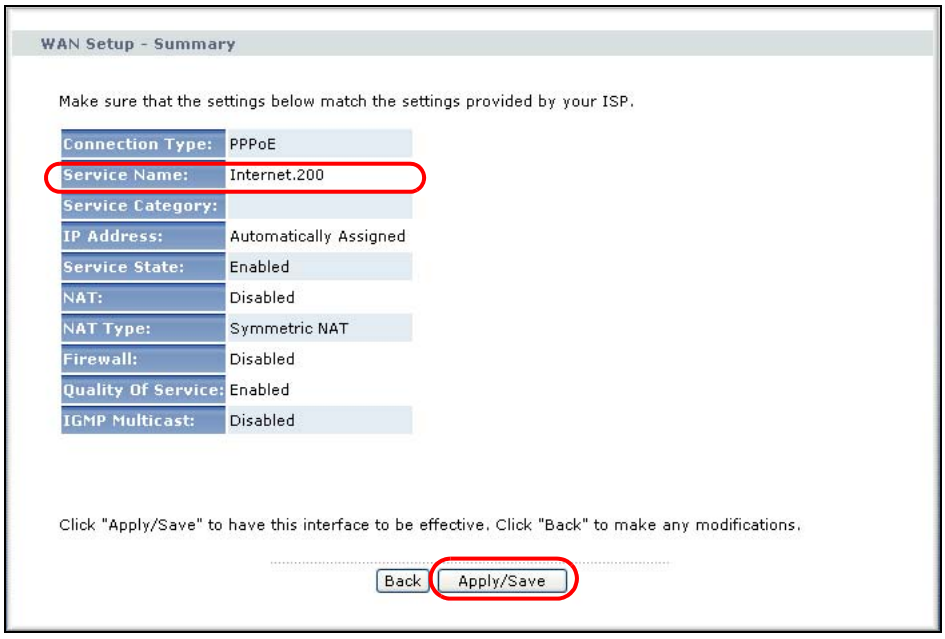
5 Remove the existing interfaces in the **Selected Default Gateway Interfaces** list. Select and move a WAN interface (**ppp1.200** in this example) to the **Selected Default Gateway Interfaces** list to use that interface as the default gateway. Click **Next**.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected(No Backup WAN fucntion support). Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
ppp1.200
->
<-
Available Routed WAN Interfaces
atm0
ptm0.100
eth4.100
Back
Next

6 Select the first option. Remove the existing interfaces in the **Selected DNS Server Interfaces** list. Select and move a WAN interface (**ppp1.200** in this example) to the **Selected DNS Server Interfaces** list to use that interface as the system DNS server. Click **Next**.

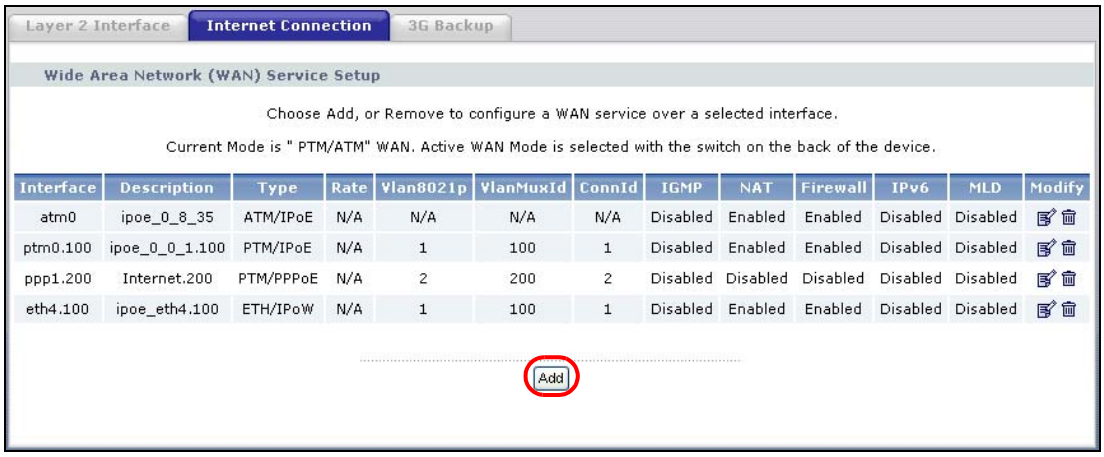

Default DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
ppp1.200
atm0
ptm0.100
eth4.100
->
<-
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Back
Next

7 The summary screen displays. The VLAN ID is appended to the service name you specified automatically. Click **Apply/Save** to save your changes and go back to the **Internet Connection** screen.

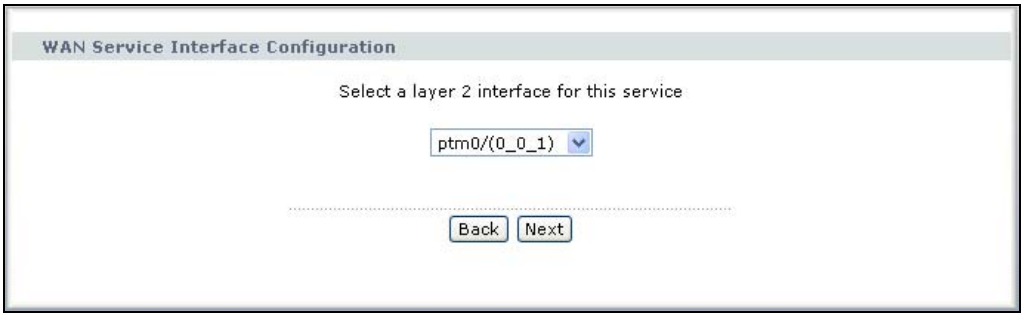

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: PPPoE
Service Name: Internet.200
Service Category:
IP Address: Automatically Assigned
Service State: Enabled
NAT: Disabled
NAT Type: Symmetric NAT
Firewall: Disabled
Quality Of Service: Enabled
IGMP Multicast: Disabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

DSL Connection for Remote Management

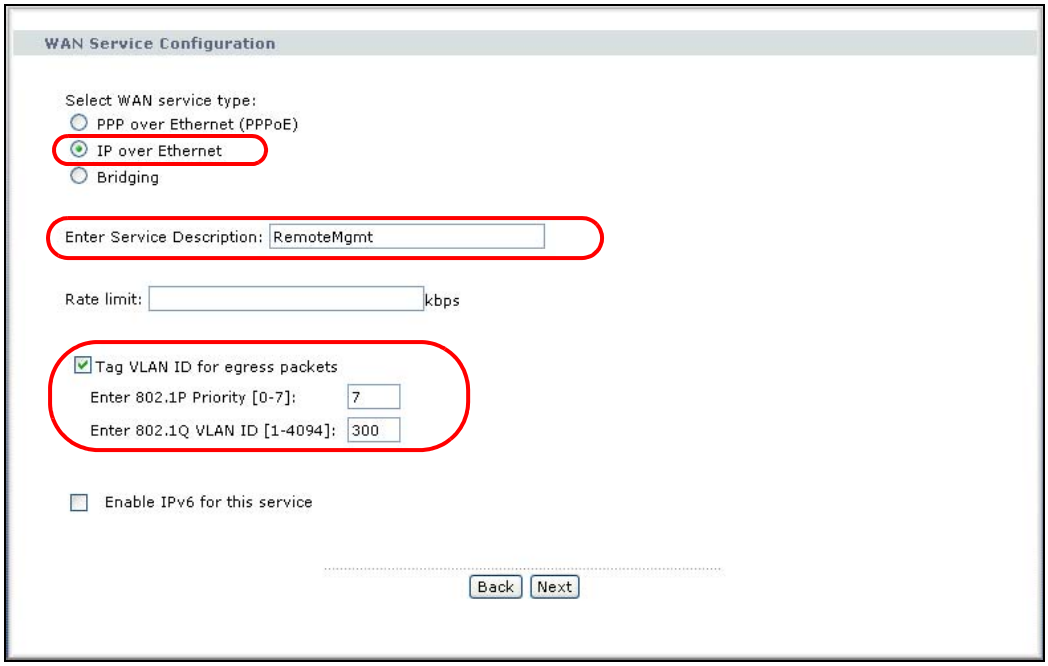
1 Go to the **WAN > Internet Connection** screen. Click **Add**.


Layer 2 Interface
Internet Connection
3G Backup
Wide Area Network (WAN) Service Setup
Choose Add, or Remove to configure a WAN service over a selected interface.
Current Mode is " PTM/ATM" WAN. Active WAN Mode is selected with the switch on the back of the device.
Interface Description Type Rate Vlan8021p VlanMuxId ConnId IGMP NAT Firewall IPv6 MLD Modify
atm0 ipoe_0_8_35 ATM/IPoE N/A N/A N/A N/A Disabled Enabled Enabled Disabled Disabled
ptm0.100 ipoe_0_0_1.100 PTM/IPoE N/A 1 100 1 Disabled Enabled Enabled Disabled Disabled
ppp1.200 Internet.200 PTM/PPPoE N/A 2 200 2 Disabled Disabled Disabled Disabled Disabled
eth4.100 ipoe_eth4.100 ETH/IPoW N/A 1 100 1 Disabled Enabled Enabled Disabled Disabled
Add

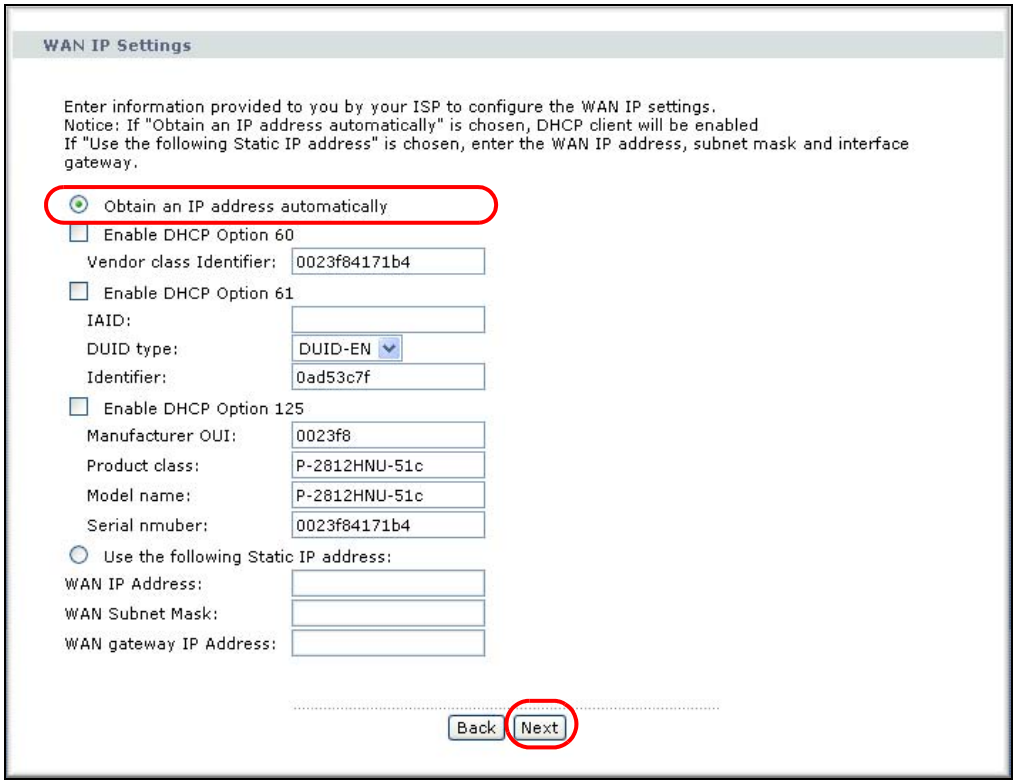
2 Select **ptm0/(0_0_1)** as the layer-2 interface. Click **Next**.



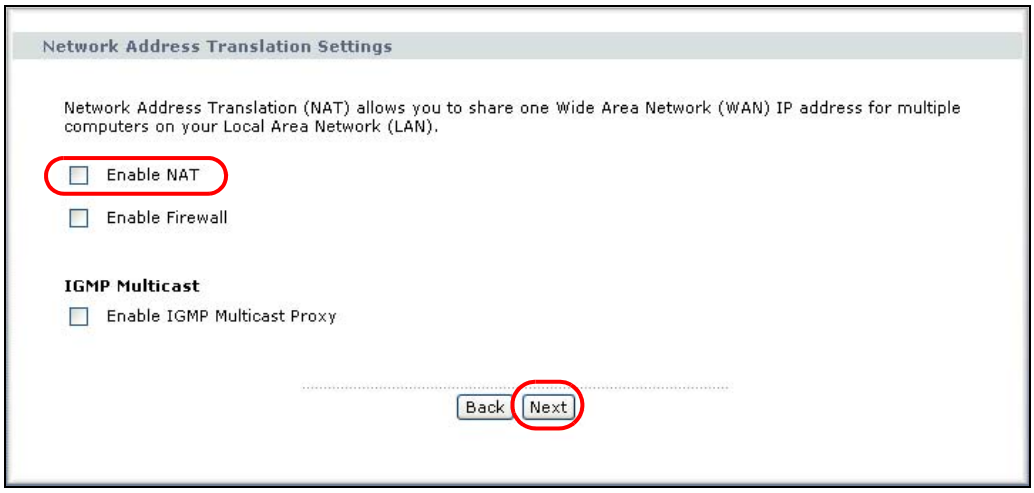
3 Select **IP over Ethernet**, enter a descriptive service name (**RemoteMgmt** in this example), and set the priority level to **7** and VLAN ID to **300**. Click **Next**.



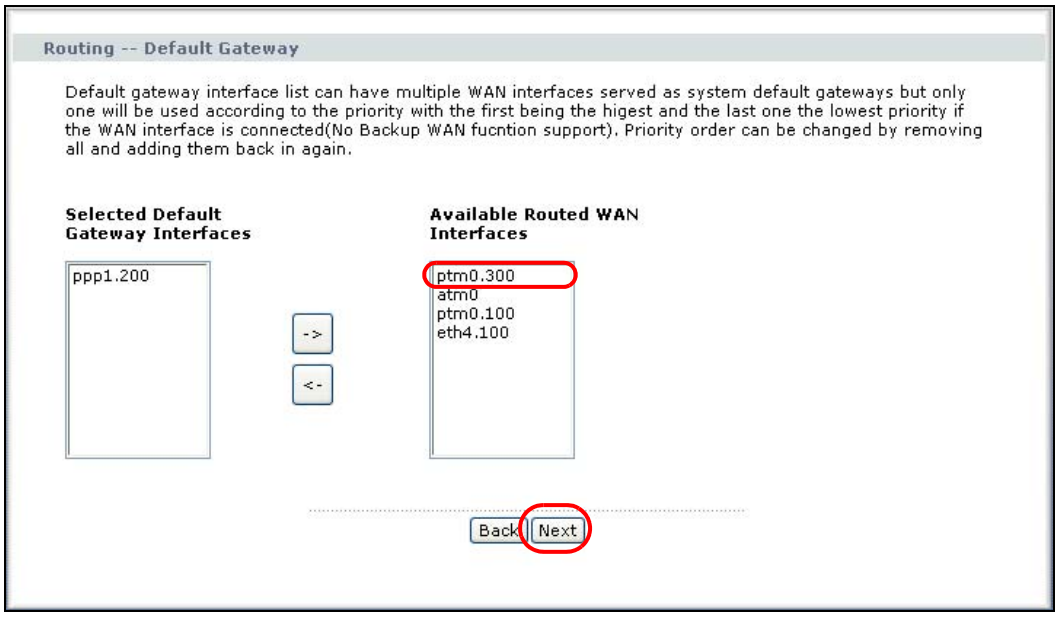
4 Select **Obtain an IP address automatically** and click **Next**.


WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP client will be enabled
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.
Obtain an IP address automatically
Enable DHCP Option 60
Vendor class Identifier: 0023f84171b4
Enable DHCP Option 61
IAID:
DUID type: DUID-EN
Identifier: 0ad53c7f
Enable DHCP Option 125
Manufacturer OUI: 0023f8
Product class: P-2812HNU-51c
Model name: P-2812HNU-51c
Serial nmuber: 0023f84171b4
Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:
Back
Next

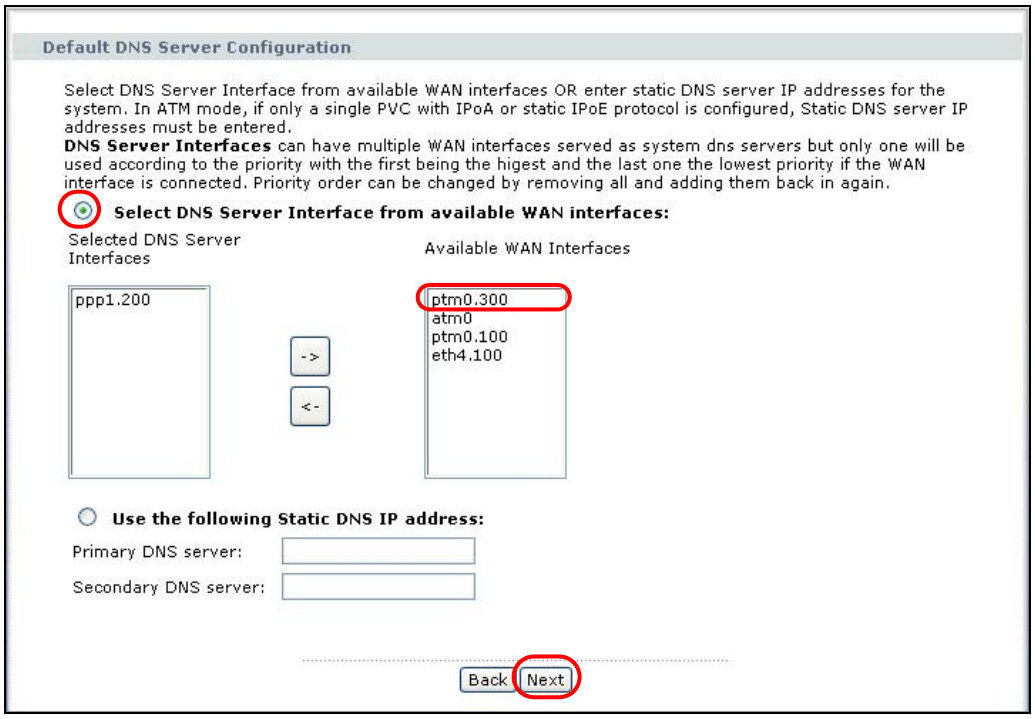
5 Make sure **Enable NAT** is not selected and click **Next**.


Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Enable Firewall
IGMP Multicast
Enable IGMP Multicast Proxy
Back
Next

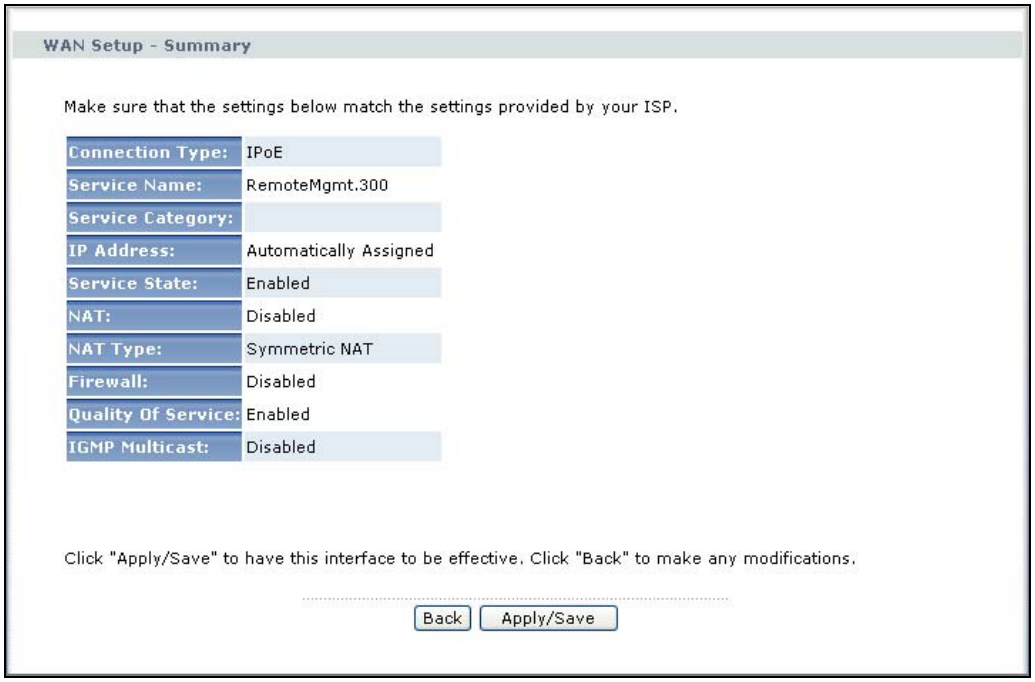
6 Keep the WAN interface (**ptm0.300** in this example) in the **Available Routed WAN Interfaces** list to not have the clients use this interface as the default gateway. Click **Next**.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected(No Backup WAN fucntion support). Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ppp1.200
->
<-
ptm0.300
atm0
ptm0.100
eth4.100
Back
Next

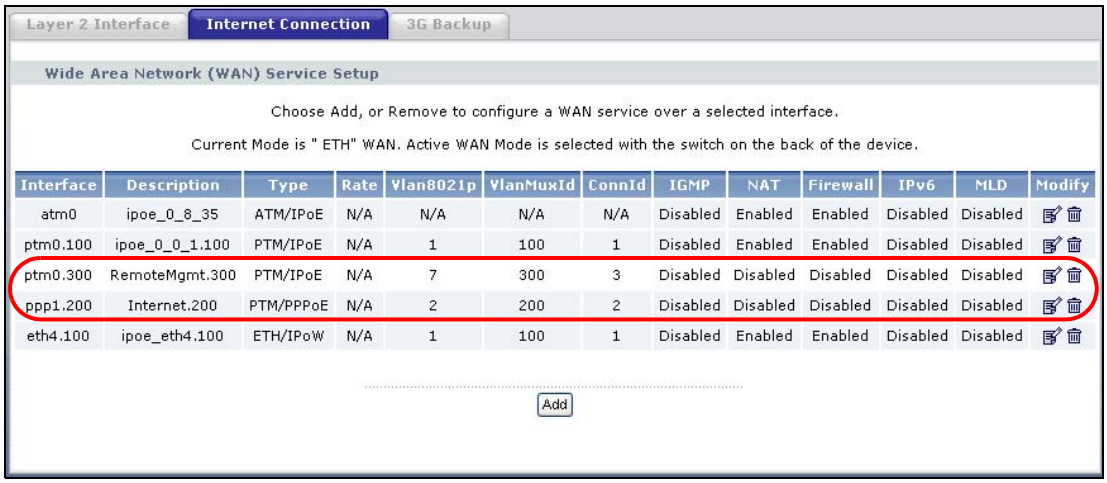
7 Select the first option. Keep the WAN interface (**ptm0.300** in this example) in the **Available WAN Interfaces** list to not have the clients use this interface as the system DNS server. Click **Next**.


Default DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
ppp1.200
ptm0.300
atm0
ptm0.100
eth4.100
->
<-
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Back
Next

8 The summary screen displays. Click **Apply/Save** to save your changes and go back to the **Internet Connection** screen. The VLAN ID is appended to the service name you specified automatically.

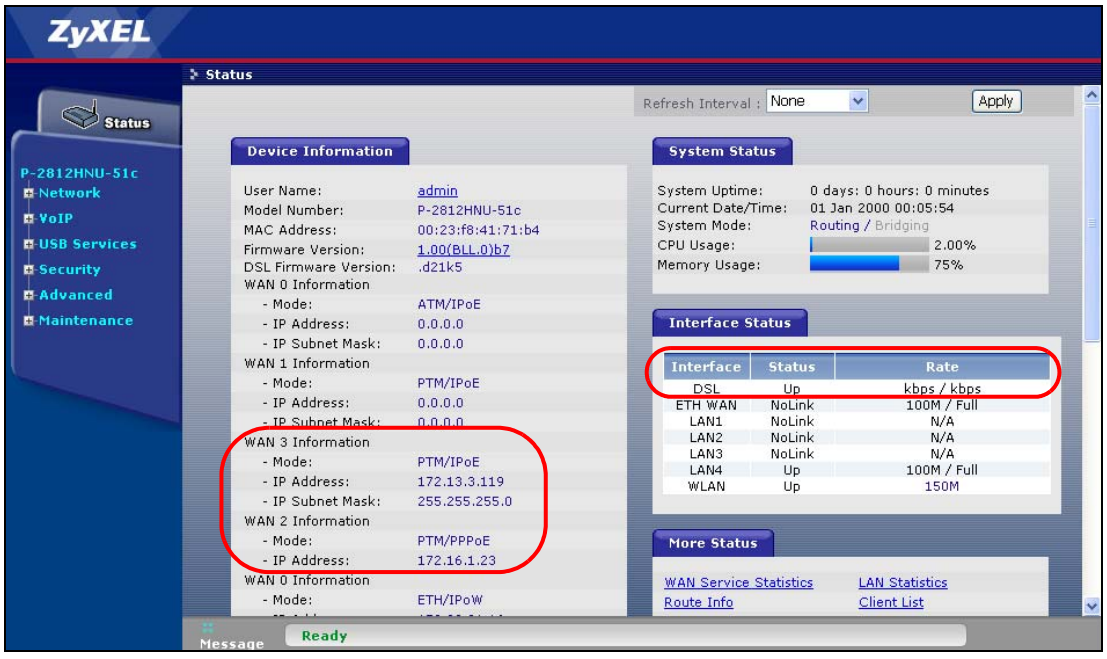

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: IPoE
Service Name: RemoteMgmt.300
Service Category:
IP Address: Automatically Assigned
Service State: Enabled
NAT: Disabled
NAT Type: Symmetric NAT
Firewall: Disabled
Quality Of Service: Enabled
IGMP Multicast: Disabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

9 The **Internet Connection** screen should look like the following.


Layer 2 Interface
Internet Connection
3G Backup
Wide Area Network (WAN) Service Setup
Choose Add, or Remove to configure a WAN service over a selected interface.
Current Mode is " ETH" WAN. Active WAN Mode is selected with the switch on the back of the device.
Interface Description Type Rate Vlan8021p VlanMuxId ConnId IGMP NAT Firewall IPv6 MLD Modify
atm0 ipoe_0_8_35 ATM/IPoE N/A N/A N/A N/A Disabled Enabled Enabled Disabled Disabled
ptm0.100 ipoe_0_0_1.100 PTM/IPoE N/A 1 100 1 Disabled Enabled Enabled Disabled Disabled
ptm0.300 RemoteMgmt.300 PTM/IPoE N/A 7 300 3 Disabled Disabled Disabled Disabled Disabled
ppp1.200 Internet.200 PTM/PPPoE N/A 2 200 2 Disabled Disabled Disabled Disabled Disabled
eth4.100 ipoe_eth4.100 ETH/IPoW N/A 1 100 1 Disabled Enabled Enabled Disabled Disabled
Add

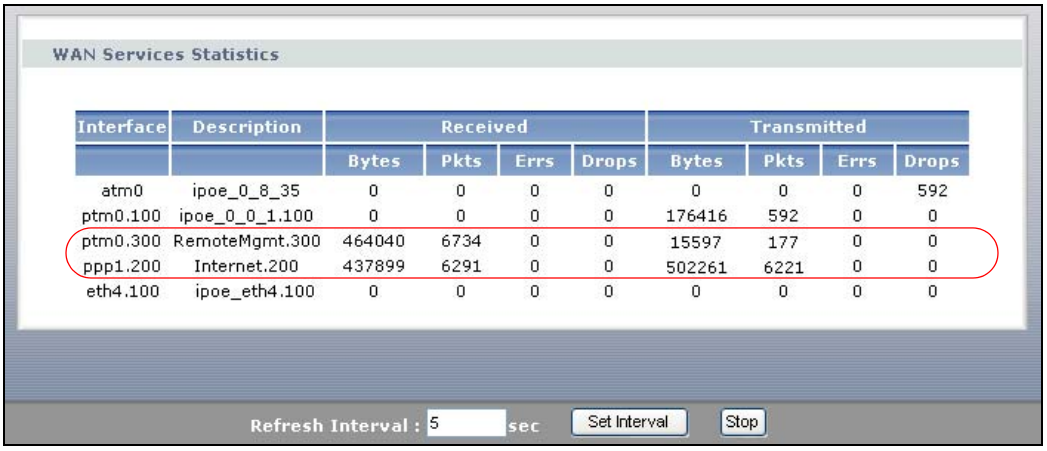
DSL Connections Status

1 Go to the **Status** screen. Check and write down the WAN IP addresses assigned by your ISP for the WAN connections in PTM mode you configured (2 and 3 in this example). Your DSL interface status should also be **Up** and display the transmission rates.



2 Click the **WAN Service Statistics** link under **More Status** in the **Status** screen.

3 The **WAN Service Ststistics** screen displays. Check if any packets are transmitted or received through the two WAN connections you just configured.

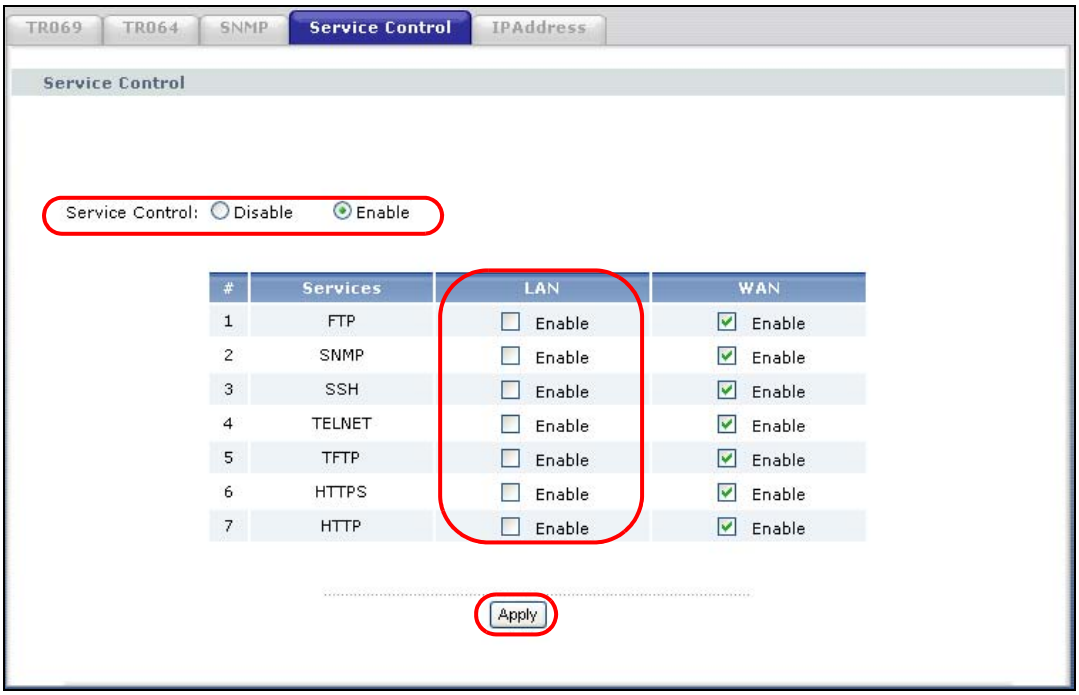


2.4.2 Configuring Remote Management

Follow the steps below to not allow access to the P-2812HNU-51c from the LAN.

1 Click **Advanced > Remote MGNT > Service Control**.

2 Select the **Enable** option, and deselect all service options in the **LAN** column. Click **Apply**.



2.4.3 Testing the Connection

After you finish all the settings in this tutorial, you would not be able to access the web configurator from the LAN anymore. Check if you can use the WAN IP address for the **RemoteMgmt** WAN connection to access the P-2812HNU-51c. You should also be able to access the Internet using the computer which is connected to the P-2812HNU-51c's LAN port.

3

Introducing the Web Configurator

3.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions or Mozilla Firefox 3 and later versions or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See Appendix C on page 445 if you need to make sure these functions are allowed in Internet Explorer.

3.1.1 Accessing the Web Configurator

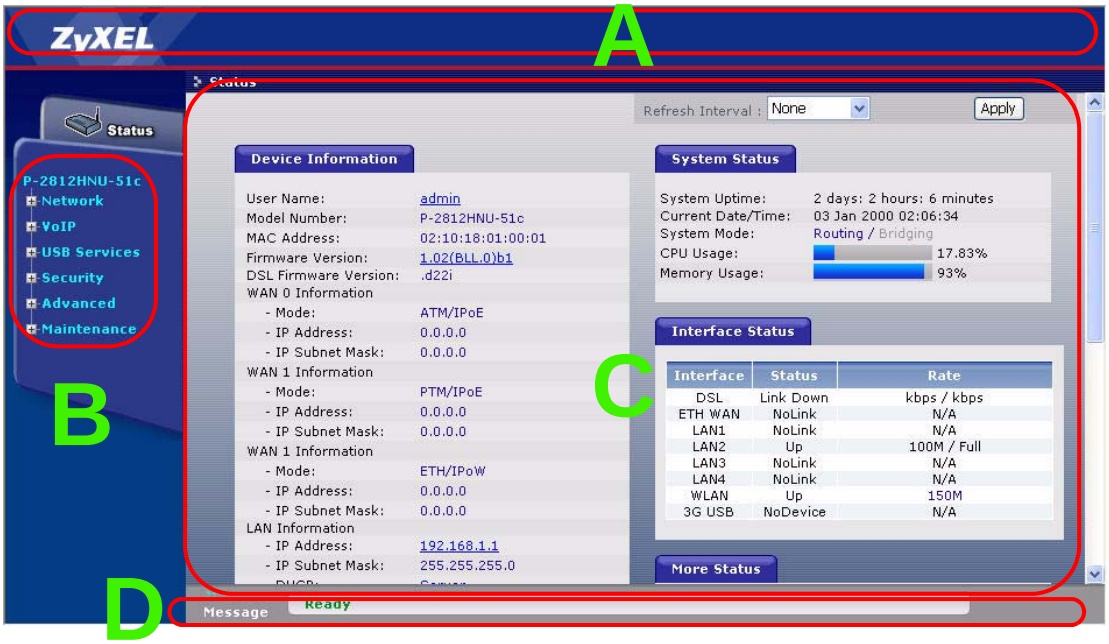
1. Make sure your P-2812HNU-51c hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "https://192.168.1.1" or "http://192.168.1.1" as the URL.

4 A password screen displays. Enter the default admin user name **admin** and default admin password **1234**. Otherwise, enter the default user name **user** and user password **user**. You cannot configure the VoIP and TR-069 settings with the user account. The password displays in non-readable characters. If you have changed the password, enter your password and click **OK**. Click **Cancel** to revert to the default password in the password field.

Figure 23 Password Screen

3.2 Web Configurator Main Screen

Figure 24 Main Screen



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

3.2.1 Navigation Panel

Use the menu items on the navigation panel to open screens to configure P-2812HNU-51c features. The following tables describe each menu item.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen shows the P-2812HNU-51c's general device and network status information. Use this screen to access the statistics and client list.
Network		
WAN	Layer 2 Interface	Use this screen to add or remove an ATM, PTM or Ethernet layer-2 interface.
	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, and other advanced properties.
	3G Backup	Use this screen to configure the 3G WAN connection.
LAN	IP	Use this screen to configure LAN TCP/IP, DHCP and IP alias settings.
	IPv6	Use this screen to configure the IPv6 settings for your P-2812HNU-51c LAN interface.
Wireless LAN	General	Use this screen to configure the wireless LAN settings, WLAN authentication/security settings and MAC filtering rules.
	More AP	Use this screen to configure multiple BSSs on the P-2812HNU-51c.
	WPS	Use this screen to enable WPS (Wi-Fi Protected Setup) and view the WPS status.
	WPS Station	Use this screen to use WPS to set up your wireless network.
	WDS	Use this screen to set up Wireless Distribution System links to other access points.
	Scheduling	Use this screen to configure the times your wireless LAN is turned off.
	Advanced Setup	Use this screen to configure the advanced wireless LAN settings.
NAT	Port Forwarding	The **NAT** screens are available only when you enable NAT in a WAN connection. Use this screen to make your local servers visible to the outside world.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
	Trigger Port	Use this screen to change your P-2812HNU-51c's port triggering settings.
	DMZ Host	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to allow SIP sessions to pass through the P-2812HNU-51c.
VoIP		
SIP	SIP Account	Use this screen to configure your P-2812HNU-51c's Voice over IP settings. Use this screen to set which phone ports use which SIP accounts.
	SIP Service Provider	Use this screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions and dialing plan
Phone	Region	Use this screen to select your location and call service mode.
Phone Book	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
Call History	Call History Summary	Use this screen to view the summary list of received, dialed and missed calls.
	Outgoing Calls	Use this screen to view detailed information for each outgoing call you made
	Incoming Calls	Use this screen to view detailed information for each incoming call from someone calling you.
USB Services		
File Sharing	Share Configuration	Use this screen to enable file sharing via the P-2812HNU-51c.
Print Server	Printer Configuration	Use this screen to enable the print server on the P-2812HNU-51c and get the model name of the associated printer.
Security		
IPSec	IPSec	Use this screen to view the configured VPN policies and add, edit or remove a VPN policy.
	Status	Use this screen to view and manage the current active VPN connections.
Firewall	Incoming	This screen shows a summary of the IP filtering rules, and allows you to add or remove an incoming IP filtering rule that allows incoming traffic from the WAN.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
Advanced		
Static Route	IP Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Policy Forwarding		Use this screen to configure policy routing on the P-2812HNU-51c.
DNS Route		Use this screen to view and configure DNS routes.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
RIP		Use this screen to configure RIP (Routing Information Protocol) settings.
QoS	General	Use this screen to enable QoS and set bandwidth.
	Queue Setup	Use this screen to configure QoS queues.
	Class Setup	Use this screen to define a classifier.
	Policer Setup	Use these screens to configure QoS policers.
	Monitor	Use this screen to view QoS packets statistics.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.
Remote MGMT	TR069	Use this screen to configure the P-2812HNU-51c to be managed by an ACS (Auto Configuration Server).
	TR064	Use this screen to enable management via TR-064 on the LAN.
	SNMP	Use this screen to to configure your P-2812HNU-51c's settings for Simple Network Management Protocol management.
	ServiceControl	Use this screen to configure which services/protocols can access which P-2812HNU-51c interface.
	IPAddress	Use this screen to configure from which IP address(es) users can manage the P-2812HNU-51c.
UPnP	General	Use this screen to turn UPnP on or off.
Parental Control	Time Restriction	Use this screen to configure the days and times when the restrictions are enforced.
	URL Filter	Use this screen to prevent users of your netowrk from viewing inappropriate web content.
Interface Group		Use this screen to map a port to a PVC or bridge group.
Email Notification		Use this screen to configure up to two mail servers and sender addresses on the P-2812HNU-51c.
Maintenance		
System	General	Use this screen to configure your device's name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your P-2812HNU-51c's time and date.
Logs	View Log	Use this screen to view the logs for the level that you selected.
	Log Settings	Use this screen to change your P-2812HNU-51c's log settings.
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the P-2812HNU-51c without turning the power off.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
Diagnostic	General	Use this screen to test the connections to other devices.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.
	OAM Ping Test	These screen displays information to help you identify problems with the DSL connection.

3.2.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See Chapter 4 on page 81 for more information about the **Status** screen.

3.2.3 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

PART II
Technical Reference

4

Status Screens

4.1 Overview

Use the **Status** screens to look at the current status of the device, system resources and interfaces (LAN, WAN and WLAN). The **Status** screen also provides detailed information from DHCP and statistics from traffic.

4.2 Status Screen

Click **Status** to open this screen.

Figure 25 Status Screen

Each field is described in the following table.

Table 7 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the P-2812HNU-51c to update this screen.
Apply	Click this to update this screen immediately.

Table 7 Status Screen

LABEL	DESCRIPTION
Device Information	
User Name	This field displays the P-2812HNU-51c system name. It is used for identification. Click this to go to the screen where you can change it.
Model Number	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your P-2812HNU-51c.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
DSL Firmware Version	This field displays the current version of the device's DSL modem code.
WAN Information	
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IPv4 address of the P-2812HNU-51c in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
IPv6 Address/ Mask	This field displays the current IPv6 address and prefix length for the P-2812HNU-51c's WAN interface.
IPv6 Scope	This field displays whether the IPv6 address is a link-local or global address.
LAN Information	
IP Address	This field displays the current IPv4 address of the P-2812HNU-51c in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
IPv6 Address/ Mask	This field displays the current IPv6 address and prefix length for the P-2812HNU-51c's LAN interface.
IPv6 Scope	This field displays whether the IPv6 address is a link-local or global address.

Table 7 Status Screen

LABEL	DESCRIPTION
DHCP	This field displays what DHCP services the P-2812HNU-51c is providing to the LAN. Choices are: **Server** - The P-2812HNU-51c is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The P-2812HNU-51c acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The P-2812HNU-51c is not providing any DHCP services to the LAN. Click this to go to the screen where you can change it.
WLAN Information	
Channel	This is the channel number used by the P-2812HNU-51c now.
WPS Status	This field displays the status of WPS (Wi-Fi Protected Setup). Click this to go to the screen where you can change it.
WDS Status	This field displays • **AP** when WDS is disabled. • **Bridge** when the P-2812HNU-51c functions as a wireless network bridge only to use WDS (Wireless Distribution System) to establish wireless links with other APs. • **AP+Bridge** when WDS is enabled and the P-2812HNU-51c acts as a bridge and access point simultaneously. Click this to go to the screen where you can change it
AP Information	
ESSID	This is the descriptive name used to identify the P-2812HNU-51c in this wireless network. Click this to go to the screen where you can change it.
Status	This shows the current status of the wireless network.
Security	This shows the level of wireless security the P-2812HNU-51c is using in this wireless network.
System Status	
System Uptime	This field displays how long the P-2812HNU-51c has been running since it last started up. The P-2812HNU-51c starts up when you plug it in, when you restart it (**Maintenance > Tools > Restart**), or when you reset it (see Section 1.5 on page 29).
Current Date/Time	This field displays the current date and time in the P-2812HNU-51c. You can change this in **Maintenance > System > Time Setting**.
System Mode	This displays whether the P-2812HNU-51c is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the P-2812HNU-51c's processing ability is currently used. When this percentage is close to 100%, the P-2812HNU-51c is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 19 on page 307).

Table 7 Status Screen

LABEL	DESCRIPTION
Memory Usage	This field displays what percentage of the P-2812HNU-51c's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the P-2812HNU-51c is probably becoming unstable, and you should restart the device. See Section 28.4 on page 376, or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the P-2812HNU-51c has.
Status	This field indicates whether or not the P-2812HNU-51c is using the interface. For the DSL interface, this field displays **LinkDown** (line is down) or **Up** (line is up or connected). For the LAN or Ethernet WAN interface, this field displays **Up** when the P-2812HNU-51c is using the interface and **NoLink** when the line is disconnected. For the WLAN interface, it displays **Up** when WLAN is enabled or **Disabled** when WLAN is not active. For the 3G WAN interface, it displays: • **NoDevice** when no 3G card is inserted, • **Disabled** when the 3G WAN is not activated, • **Up** when the 3G WAN connection is up, • **Down** when the 3G connection is down, • **NoResponse** when there is no response from the inserted 3G card, • **NeedPIN** if the PIN code you entered in the **WAN > 3G Backup** screen is not the right one for the 3G card you inserted, • **NeedPUK** if you enter the PIN (Personal Identification Number) code incorrectly for three times and the SIM card is blocked by your ISP, • or **DamagedSIM** when the SIM card is damaged or not inserted. If a link displays in this field, click the link to view more status information or enter the correct PIN or PUK (Personal Unblocking Key) code.
Rate	For the DSL interface, it displays the downstream and upstream transmission rate. For the LAN or Ethernet WAN interface, this displays the port speed and duplex setting. For the WLAN interface, it displays the maximum transmission rate. For the 3G WAN interface, it displays the downstream and upstream transmission rate.
More Status	
WAN Service Statistics	Click this link to view packet specific statistics of the WAN connection(s). See Section 4.2.3 on page 89.
Route Info	Click this link to view the internal routing table on the P-2812HNU-51c. See Section 4.2.4 on page 90.

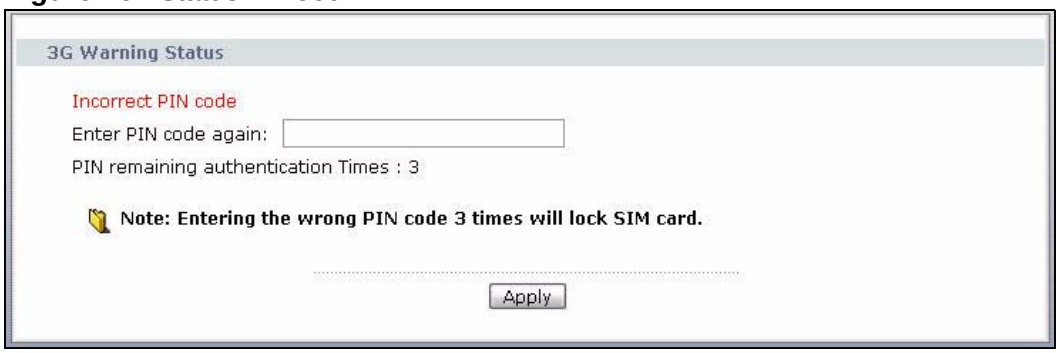
Table 7 Status Screen

LABEL	DESCRIPTION
VoIP Status	Click this link to view status of your VoIP usage. See Section 4.3.1 on page 94.
WLAN Station List	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the P-2812HNU-51c. See Section 4.3.1 on page 94.
LAN Statistics	Click this link to view packet specific statistics on the LAN and WLAN interfaces. See Section 4.3.2 on page 95.
Client List	Click this link to view current DHCP client information. See Section 4.3.3 on page 96.
Registration Status	
Account	This column displays each SIP account in the P-2812HNU-51c.
Service-Provider/SIP Account Number	This column displays the service provider name and SIP number for each SIP account.
Action	If the SIP account is already registered with the SIP server, the **Account Status** field displays **Registered**. • Click **Unregister** to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. If the SIP account is not registered with the SIP server, the **Account Status** field displays **Not Registered**. • Click **Register** to have the P-2812HNU-51c attempt to register the SIP account with the SIP server. The button is grayed out if the SIP account is disabled.
Account Status	This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Account**. **Not Registered** - The last time the P-2812HNU-51c tried to register the SIP account with the SIP server, the attempt failed. Use the **Register** button to register the account again. The P-2812HNU-51c automatically tries to register the SIP account when you turn on the P-2812HNU-51c or when you activate it. **Registered** - The SIP account is already registered with the SIP server. You can use it to make a VoIP call.
URI	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP > SIP** screens.

4.2.1 3G Status: NeedPIN

Click the **NeedPIN** link under **Interface Status** of the **Status** screen to access this screen. Use this screen to enter the right PIN code for your 3G card.

Figure 26 Status > Need PIN


3G Warning Status
Incorrect PIN code
Enter PIN code again:
PIN remaining authentication Times : 3
Note: Entering the wrong PIN code 3 times will lock SIM card.
Apply

The following table describes the labels in this screen.

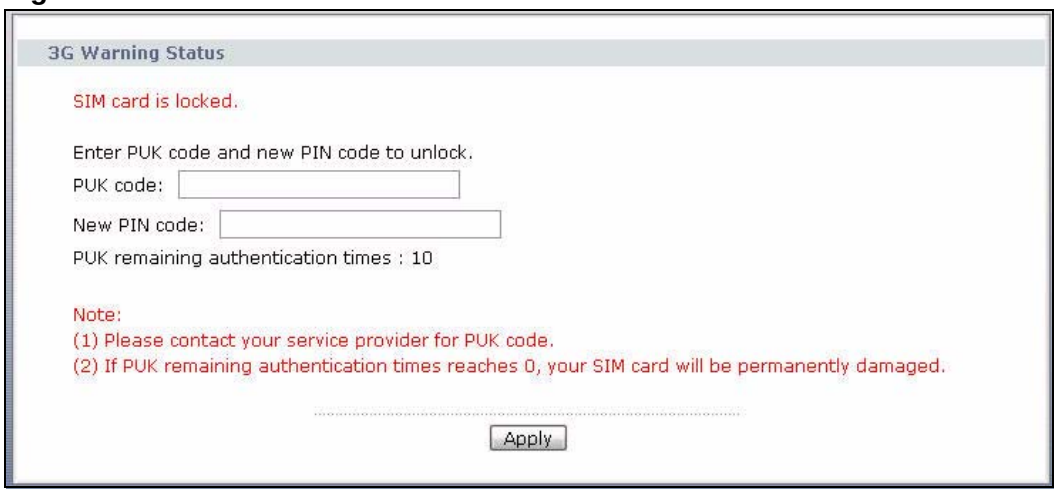
Table 8 Status > Need PIN

LABEL	DESCRIPTION
Enter PIN code again	Enter the correct PIN code (four to eight digits) for the inserted 3G card.
PIN remaining authentication times	This field displays how many times you can still enter a wrong PIN code before your ISP blocks your SIM card.
Apply	Click **Apply** to save the correct PIN code and replace the one you specified in the **3G Backup** screen.

4.2.2 3G Status: NeedPUK

Click the **NeedPUK** link under **Interface Status** of the **Status** screen to access this screen. Use this screen to enter the PUK code to enable the 3G SIM card again.

Figure 27 Status > Need PUK


3G Warning Status
SIM card is locked.
Enter PUK code and new PIN code to unlock.
PUK code:
New PIN code:
PUK remaining authentication times : 10
Note:
(1) Please contact your service provider for PUK code.
(2) If PUK remaining authentication times reaches 0, your SIM card will be permanently damaged.
Apply

The following table describes the labels in this screen.

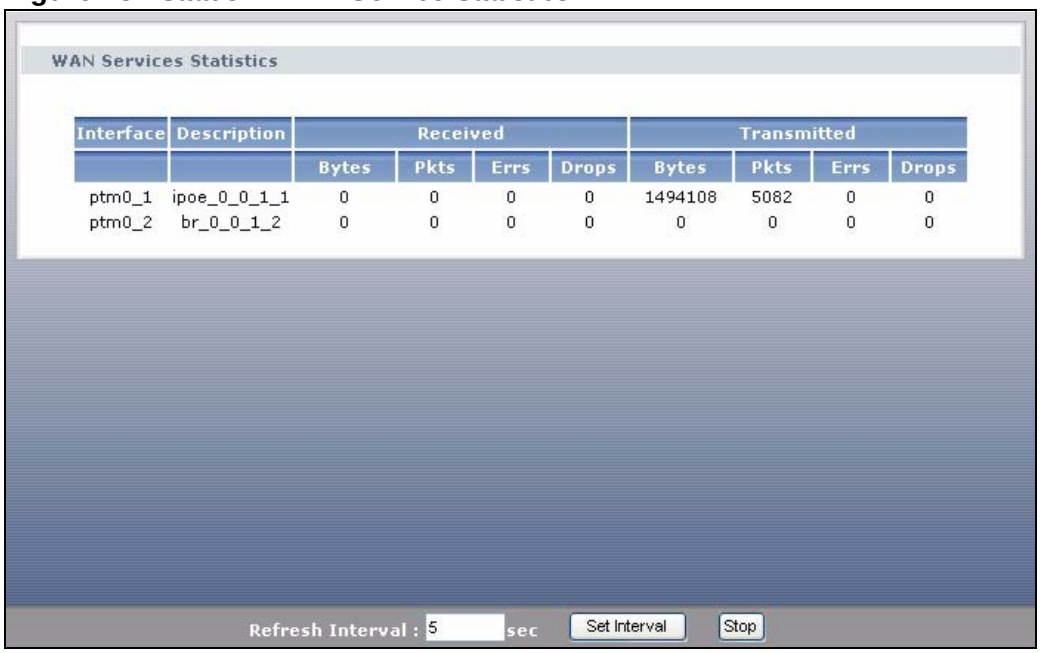
Table 9 Status > Need PUK

LABEL	DESCRIPTION
PUK code	If you enter the PIN code incorrectly three times, the SIM card will be blocked by your ISP and you cannot use the account to access the Internet. You should get the PUK (Personal Unblocking Key) code (four to eight digits) from your ISP. Enter the PUK code to enable the SIM card. If an incorrect PUK code is entered 10 times, the SIM card will be disabled permanently. You then need to contact your ISP for a new SIM card.
New PIN code	Configure a PIN code for the SIM card. You can specify any four to eight digits to have a new PIN code or enter the previous PIN code.
PUK remaining authentication times	This field displays how many times you can still enter a wrong PUK code before your ISP disables your SIM card permanently.
Apply	Click **Apply** to save your changes to the P-2812HNU-51c.

4.2.3 WAN Service Statistics

Click **Status > WLAN Service Statistics** to access this screen. Use this screen to view the WAN statistics.

Figure 28 Status > WAN Service Statistics



The following table describes the labels in this screen.

Table 10 Status > WAN Service Statistics

LABEL	DESCRIPTION
Interface	This shows the name of the WAN interface used by this connection. A default name **ipoax**, **atmx** (where x starts from 0 and is the index number of ATM layer-2 interfaces using different VPI and/or VCI values) or **ptm0** indicates the DSL port. The **pppx** name (where x starts from 1 and is the index number of PPP connection on the P-2812HNU-51c) indicates a PPP connection via any one of the WAN interface. **eth4** indicates the Ethernet WAN interface (the physical Ethernet WAN port). The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (_) represents the index number of connections through the same interface. **(null)** means the entry is not valid.
Description	This shows the descriptive name of this connection. **8** and **35** or **0** and **1** are the default VPI and VCI numbers. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection. **(null)** means the entry is not valid.
Received	

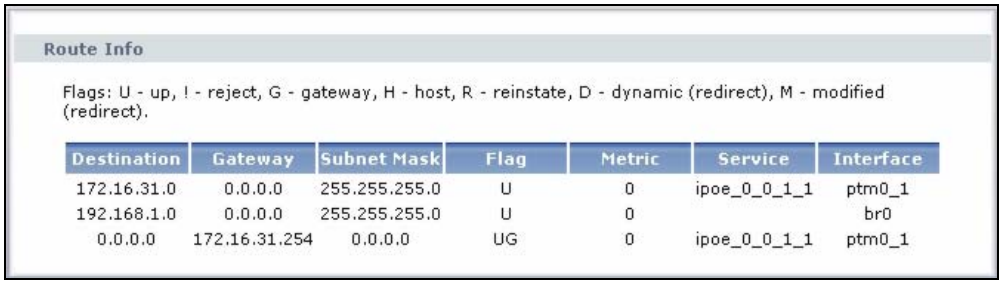
Table 10 Status > WAN Service Statistics (continued)

LABEL	DESCRIPTION
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.
Drops	This indicates the number of outgoing packets dropped on this interface.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.

4.2.4 Route Info

Routing is based on the destination address only and the P-2812HNU-51c takes the shortest path to forward a packet. Click **Status > Route Info** to access this screen. Use this screen to view the internal routing table on the P-2812HNU-51c.

Figure 29 Status > Route Info


Route Info
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect).
Destination Gateway Subnet Mask Flag Metric Service Interface
172.16.31.0 0.0.0.0 255.255.255.0 U 0 ipoe_0_0_1_1 ptm0_1
192.168.1.0 0.0.0.0 255.255.255.0 U 0 br0
0.0.0.0 172.16.31.254 0.0.0.0 UG 0 ipoe_0_0_1_1 ptm0_1

The following table describes the labels in this screen.

Table 11 Status > Route Info

LABEL	DESCRIPTION
Destination	This indicates the destination IP address of this route.
Gateway	This indicates the IP address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of this route.

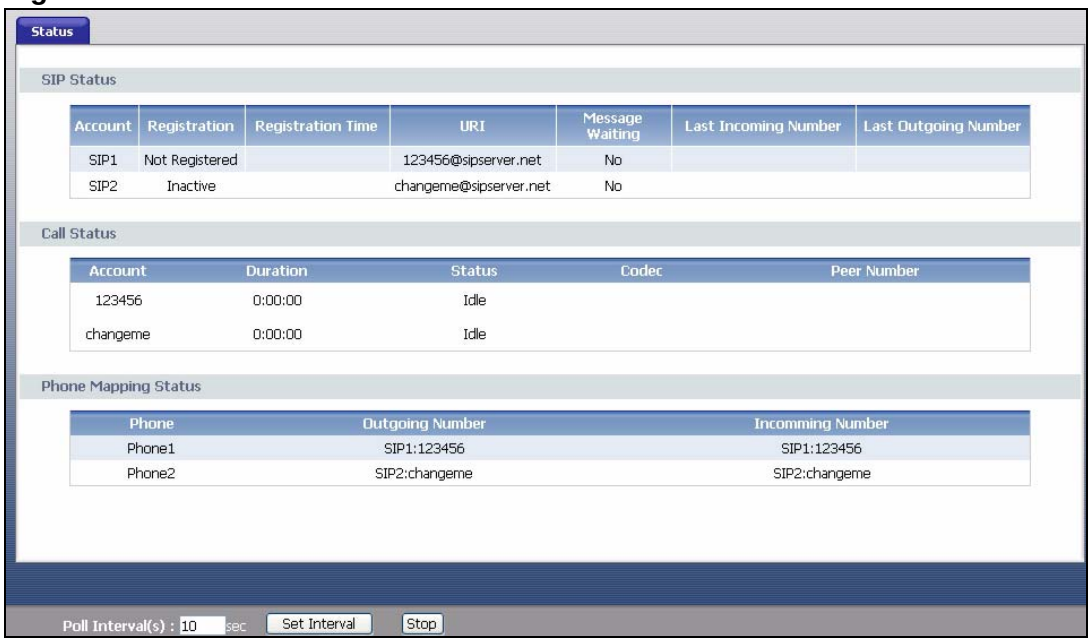
Table 11 Status > Route Info (continued)

LABEL	DESCRIPTION
Flag	This indicates the route status. **U**p: The route is up. **!**(Reject): The route is blocked and will force a route lookup to fail. **G**ateway: The route uses a gateway to forward traffic. **H**ost: The target of the route is a host. **R**einstate: The route is reinstated for dynamic routing. **D**ynamic (redirect): The route is dynamically installed by a routing daemon or redirect **M**odified (redirect): The route is modified from a routing daemon or redirect.
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Service	This indicates the name of the service used to forward the route.
Interface	This indicates the name of the interface through which the route is forwarded. • **br0** indicates the LAN interface. • **ptm0** indicates the VDSL WAN interface using IPoE or in bridge mode. • **atmx** (where x starts from 0 and is the index number of ATM layer-2 interfaces using different VPI and/or VCI values) indicates the ADSL WAN interface using IPoE, PPPoA or in bridge mode. • **pppoax** indicates the ADSL WAN interface using PPPoA. • **ipoa0** indicates the ADSL WAN interface using IPoA. • **pppx** (where x starts from 1 and is the index number of PPP connection) indicates the WAN interface using PPPoE. • **eth4** indicates the Ethernet WAN interface using IPoE. • **3G** indicates the 3G WAN interface.

4.3 VoIP Status

Click **Status > VoIP Status** to access this screen.

Figure 30 VoIP Status



Each field is described in the following table.

Table 12 VoIP Status

LABEL	DESCRIPTION
SIP Status	
Account	This column displays each SIP account in the P-2812HNU-51c.
Registration	This field displays the current registration status of the SIP account. You can change this in the **Status** screen. **Registered** - The SIP account is registered with a SIP server. **Not Registered** - The last time the P-2812HNU-51c tried to register the SIP account with the SIP server, the attempt failed. The P-2812HNU-51c automatically tries to register the SIP account when you turn on the P-2812HNU-51c or when you activate it. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Account**.
Last Registration	This field displays the last time you successfully registered the SIP account. The field is blank if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP > SIP** screens.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.

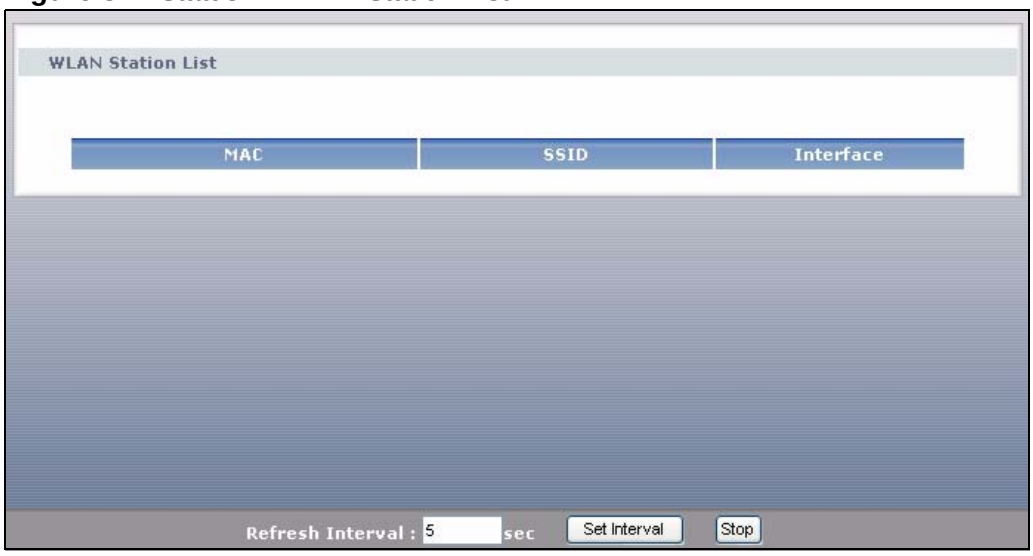
Table 12 VoIP Status

LABEL	DESCRIPTION
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the P-2812HNU-51c.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. **Idle** - There are no current VoIP calls, incoming calls or outgoing calls being made. **Dial** - The callee's phone is ringing. **Ring** - The phone is ringing for an incoming VoIP call. **Process** - There is a VoIP call in progress. **DISC** - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Mapping Status	
Phone	This field displays each phone port in the P-2812HNU-51c.
Outgoing Number	This field displays the SIP account and SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP account and SIP number that you use to receive calls on this phone port.
Poll Interval(s)	Enter how often you want the P-2812HNU-51c to update this screen, and click **Set Interval**.
Set Interval	Click this to make the P-2812HNU-51c update the screen based on the amount of time you specified in **Poll Interval**.
Stop	Click this to make the P-2812HNU-51c stop updating the screen.

4.3.1 WLAN Station List

Click **Status > WLAN Station List** to access this screen. Use this screen to view the wireless stations that are currently associated to the P-2812HNU-51c.

Figure 31 Status > WLAN Station List



The following table describes the labels in this screen.

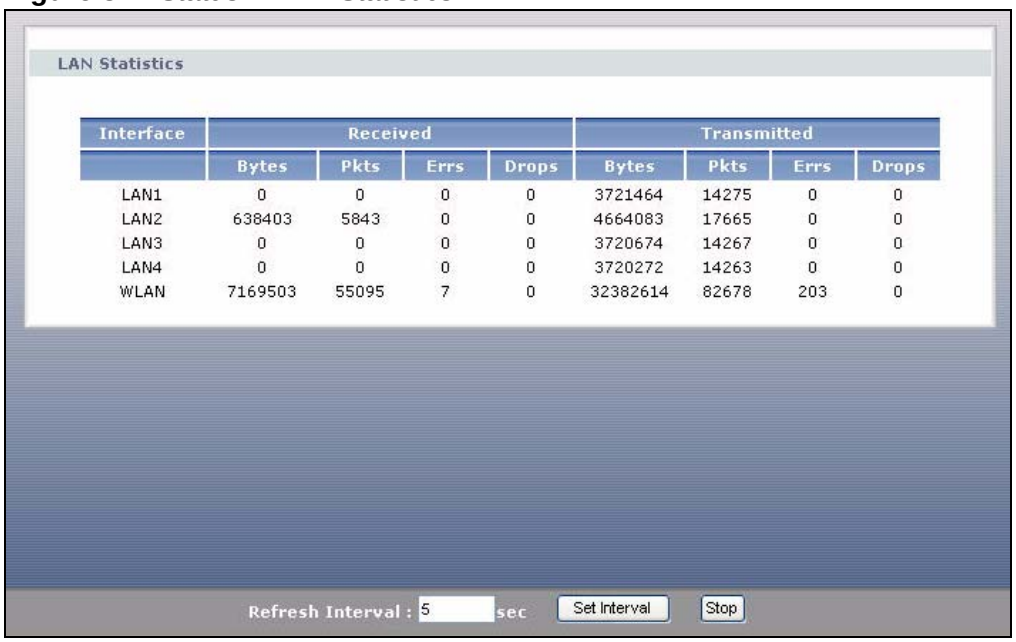
Table 13 Status > WLAN Station List

LABEL	DESCRIPTION
MAC	This field shows the MAC (Media Access Control) address of an associated wireless station.
SSID	This field shows the SSID to which the wireless station is connected.
Interface	This field shows the wireless interface to which the wireless station is connected.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.

4.3.2 LAN Statistics

Click **Status > LAN Statistics** to access this screen. Use this screen to view the LAN statistics.

Figure 32 Status > LAN Statistics



The following table describes the labels in this screen.

Table 14 Status > LAN Statistics

LABEL	DESCRIPTION
Interface	This shows the LAN or WLAN interface.
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.
Drops	This indicates the number of outgoing packets dropped on this interface.
Refresh Interval	Enter the time interval for refreshing statistics in this field.

Table 14 Status > LAN Statistics (continued)

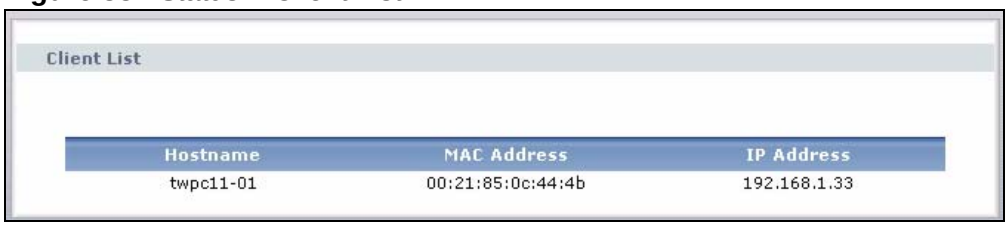
LABEL	DESCRIPTION
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.

4.3.3 Client List

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the P-2812HNU-51c as a DHCP server or disable it. When configured as a server, the P-2812HNU-51c provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Status > Client List** to open the following screen. The read-only DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the P-2812HNU-51c's DHCP server.

Figure 33 Status > Client List



The following table describes the labels in this screen.

Table 15 Status > Client List

LABEL	DESCRIPTION
Host Name	This indicates the computer host name.
MAC Address	Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. This indicates the MAC address of the client computer.
IP Address	This indicates the IP address assigned to this client computer.

5

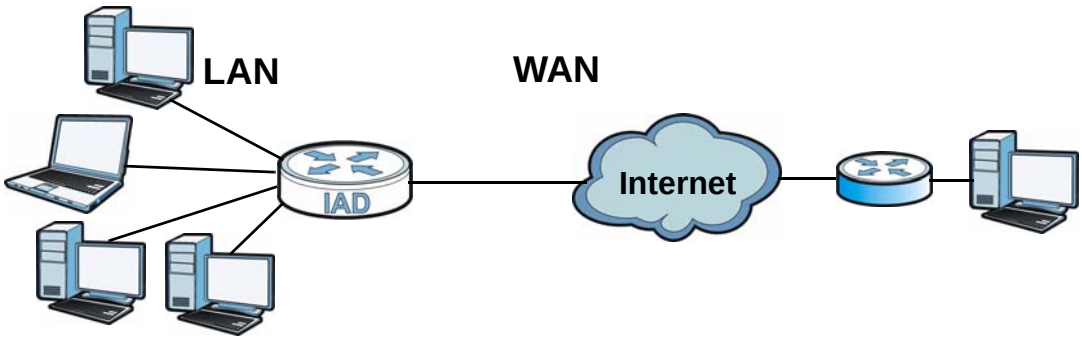
WAN Setup

5.1 Overview

This chapter discusses the P-2812HNU-51c's **WAN** screens. Use these screens to configure your P-2812HNU-51c for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network), and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 34 LAN and WAN



See Section 5.7 on page 125 for advanced technical information on WAN.

5.1.1 What You Can Do in this Chapter

- The **Layer 2 Interface** screen lets you view, remove or add a layer-2 WAN interface (Section 5.4 on page 101).

- The **Internet Connection** screen lets you view and configure the WAN settings on the P-2812HNU-51c for Internet access (Section 5.5 on page 105).

Table 16 WAN Setup Overview

LAYER-2 INTERFACE			INTERNET CONNECTION	
INTERFACE	**DSL LINK TYPE**	**CONNECTION MODE**	**WAN SERVICE TYPE**	**CONNECTION SETTINGS**
ATM	EoA	Default Mode VLAN MUX Mode MSC Mode	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
			Bridging	N/A
	PPPoA			PPP user name and password, WAN IP address, DNS server and default gateway
	IPoA			WAN IP address, NAT, DNS server and default gateway
PTM		Default Mode VLAN MUX Mode MSC Mode	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
			Bridging	N/A
Ethernet		Default Mode MSC Mode	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
		VLAN MUX Mode	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
			Bridging	N/A

- The **3G Backup** screen lets you configure the 3G WAN connection (Section 5.6 on page 122).

5.2 What You Need to Know

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPPoA, they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the P-2812HNU-51c, which makes it accessible from an outside network. It is used by the P-2812HNU-51c to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the P-2812HNU-51c tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

ATM

Asynchronous Transfer Mode (ATM) is is a LAN and WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC) between two endpoints before the actual data exchange begins.

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

NAT Types

This section discusses the following NAT types that are implemented on the P-2812HNU-51c.

- Full Cone
- Restricted Cone

- Port Restricted Cone
- Symmetric

The following table summarizes how these NAT types handle outgoing and incoming packets. Read the following sections for more details and examples.

Table 17 NAT Types

	FULL CONE	RESTRICTED CONE	PORT RESTRICTED CONE	SYMMETRIC
Incoming Packets	Any external host can send packets to the mapped external IP address and port.	Only external hosts with an IP address to which the internal host has already sent a packet can send packets to the mapped external IP address and port.	Only external hosts with an IP address and port to which the internal host has already sent a packet can send packets to the mapped external IP address and port.	A host on the external network can only send packets to the specific mapped external IP address and port that the NAT router used in sending a packet to the external host's IP address and port.
Outgoing Packets	The NAT router maps the internal IP address and port of all outgoing packets to a single IP address and port on the external network.			The NAT router maps the internal IP address and port of each outgoing packet to a different external IP address and port for each different destination IP address and port.

The examples in these NAT type sections describe NAT translation between internal (private) and external (public) IP addresses.

IPv6

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The P-2812HNU-51c supports IPv4/IPv6 dual stack and can run IPv4 and IPv6 at the same time. See Appendix F on page 483 for more information about IPv6.

3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

5.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.4 The Layer 2 Interface Screen

The P-2812HNU-51c must have a layer-2 interface to allow users to use the DSL port or Ethernet WAN port to access the Internet. The screen varies depending on the interface type you select.

Note: The ATM, PTM and Ethernet layer-2 interfaces cannot work at the same time.

Figure 35 Layer 2 Interface: PTM or Ethernet

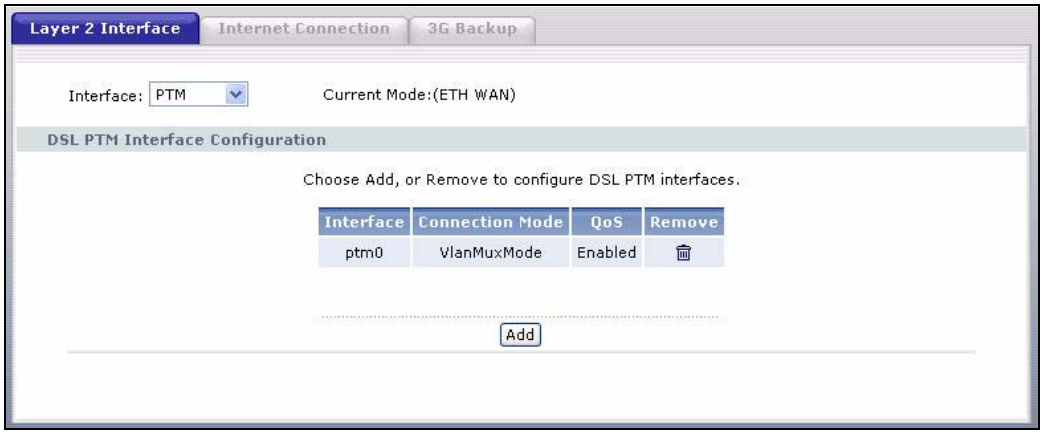
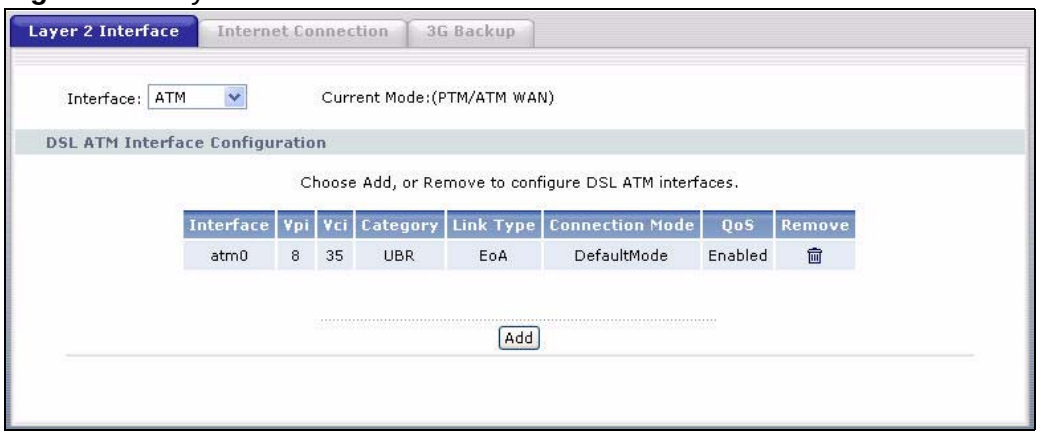


Figure 36 Layer 2 Interface: ATM



The following table describes the fields in this screen.

Table 18 Layer 2 Interface

LABEL	DESCRIPTION
Interface	Select an interface for which you want to configure here. **PTM**: The P-2812HNU-51c uses the VDSL technology for data transmission over the DSL port. **ATM**: The P-2812HNU-51c uses the ADSL technology for data transmission over the DSL port. **Ethernet**: The P-2812HNU-51c transmits data over the Ethernet WAN port. Select this if you have a DSL router or modem in your network already.
Current Mode	This displays whether the P-2812HNU-51c uses the DSL port or Ethernet WAN port for Internet access. When you set the **DSL / WAN** switch (on the back of the P-2812HNU-51c) to the **DSL** side, this displays **PTM / ATM WAN**. The **WAN** port will be disabled automatically. When you set the **DSL / WAN** switch to the **WAN** side, this displays **ETH WAN**. The **DSL** port will be disabled automatically. This allows the P-2812HNU-51c to work as an Ethernet gateway instead of a DSL router. To access the Internet, connect the **WAN** port to a broadband modem or router.
Interface	This is the name of the interface.
Vpi	This is the Virtual Path Identifier (VPI).
Vci	This is the Virtual Channel Identifier (VCI).
Category	This is the ATM traffic class.
Link Type	This is the DSL link type of the ATM layer-2 interface.
Connection Mode	This displays the connection mode of the layer-2 interface.
QoS	This displays whether QoS (Quality of Service) is enabled on the P-2812HNU-51c.
Remove	Click the **Remove** button to delete this interface from the P-2812HNU-51c. A window displays asking you to confirm that you want to delete the interface. Note: You cannot remove the layer-2 interface when a WAN service is associated with it.
Add	Click this button to create a new layer-2 interface.

5.4.1 Layer 2 Interface Configuration

Click the **Add** button in the **Layer 2 Interface** screen to open the following screen. Use this screen to create a new layer-2 interface. At the time of writing, you can configure only one PTM or Ethernet layer-2 interface on the P-2812HNU-

51c. You can have multiple ATM layer-2 interfaces using different VPI and/or VCI values. The screen varies depending on the interface type you select.

Figure 37 Layer 2 Interface Configuration: DSL ATM

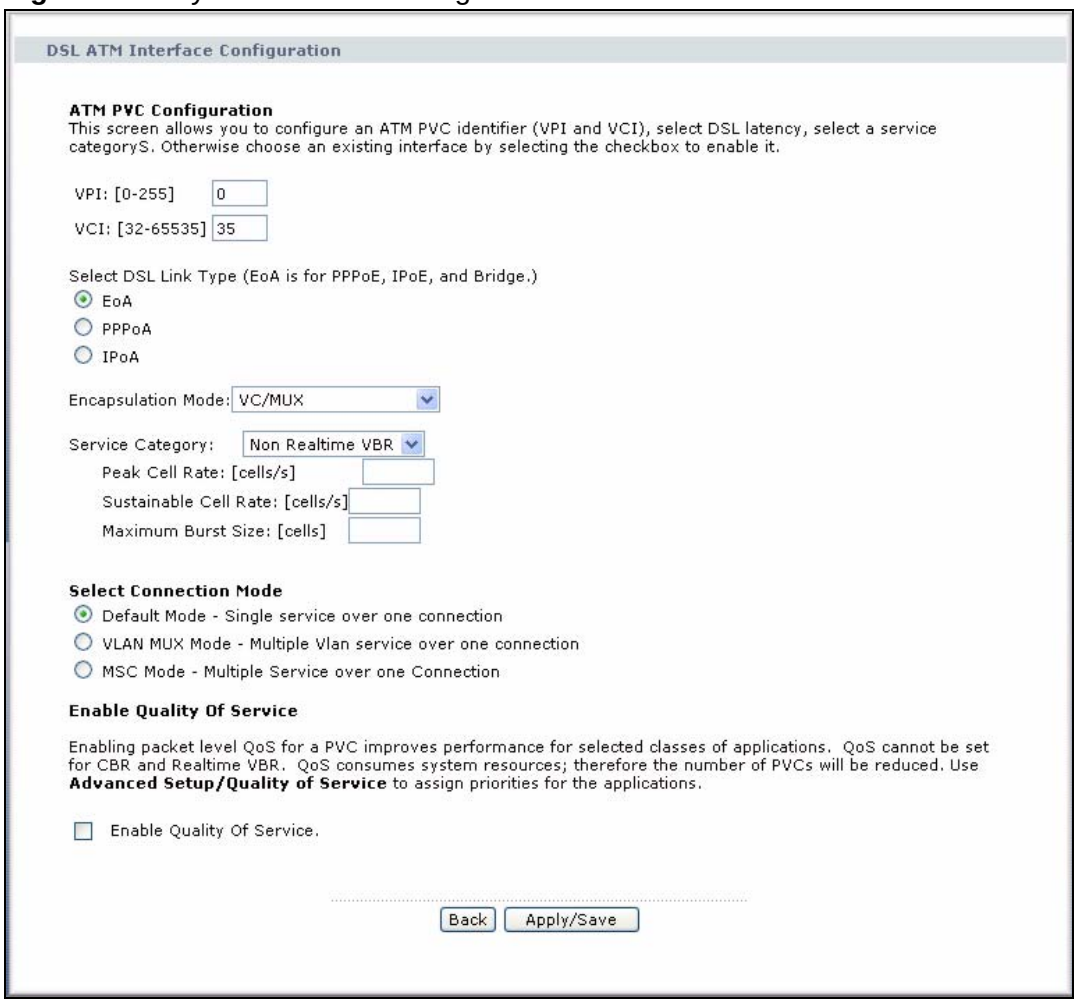

DSL ATM Interface Configuration
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 0
VCI: [32-65535] 35
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
EoA
PPPoA
IPoA
Encapsulation Mode: VC/MUX
Service Category: Non Realtime VBR
Peak Cell Rate: [cells/s]
Sustainable Cell Rate: [cells/s]
Maximum Burst Size: [cells]
Select Connection Mode
Default Mode - Single service over one connection
VLAN MUX Mode - Multiple Vlan service over one connection
MSC Mode - Multiple Service over one Connection
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service.
Back
Apply/Save

Figure 38 Layer 2 Interface Configuration: DSL PTM/Ethernet WAN

DSL PTM Interface Configuration
Select Connection Mode
Default Mode - Single service over one connection
VLAN MUX Mode - Multiple Vlan service over one connection
MSC Mode - Multiple Service over one Connection
Enable Quality Of Service
Enabling packet level QoS for this PTM interface. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service.
Back
Apply/Save

The following table describes the fields in this screen.

Table 19 Layer 2 Interface Configuration

LABEL	DESCRIPTION
ATM PVC Configuration	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. This section is available only when you configure an ATM layer-2 interface.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
Select DSL Link Type	Select **EoA** (Ethernet over ATM) to have an Ethenet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. **EoA** supports ENET ENCAP (IPoE), PPPoE and RFC1483/2684 bridging encapsulation methods. Select **PPPoA** (PPP over ATM) to allow just one PPPoA connection over a PVC. Select **IPoA** (IP over ATM) to allow just one RFC 1483 routing connection over a PVC.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list. Choices are: • **VC/MUX**: In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the P-2812HNU-51c needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload. • **LLC/ENCAPSULATION**: More than one protocol can be carried over the same VC. This is available only when you select **PPPoA** in the **Select DSL Link Type** field. • **LLC/SNAP-ROUTING**: In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LCC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select **IPoA** in the **Select DSL Link Type** field. • **LLC/SNAP-BRIDGING**: In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select **EoA** in the **Select DSL Link Type** field.
Service Category	Select **UBR Without PCR** or **UBR With PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.

Table 19 Layer 2 Interface Configuration (continued)

LABEL	DESCRIPTION
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here. This field is not available when you select **UBR Without PCR**.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Select Connection Mode	Select **Default Mode** to allow only one WAN service over a single virtual circuit. Select **MSC Mode** to allow multiple WAN services over a single virtual circuit. Each WAN connection has its own MAC address. Select **VLAN MUX Mode** to allow multiplexing of multiple protocols over a single virtual circuit. You need to assign a VLAN ID and priority level to traffic through each WAN connection. All WAN connections share one MAC address. This field is not available if you select **PPPoA** or **IPoA** as the DSL link type. The P-2812HNU-51c uses **Default Mode** automatically for **PPPoA** or **IPoA**.
Enable Quality Of Service	Select this option to activate QoS (Quality of Service) on this interface to group and prioritize traffic. Traffic is grouped according to the VLAN group. The QoS setting applies to all WAN connections over the same PVC. This field is not available when you select **CBR** or **Realtime VBR**.
Back	Click this button to return to the previous screen without saving any changes.
Apply/Save	Click this button to save your changes and go back to the previous screen.

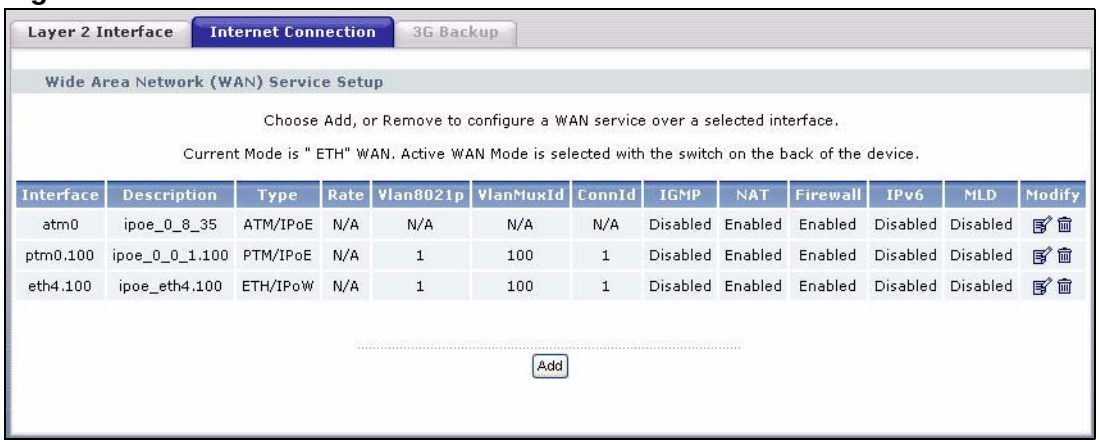
5.5 The Internet Connection Screen

Use this screen to change your P-2812HNU-51c's WAN settings. Click **Network > WAN > Internet Connection**. The summary table shows you the configured WAN services (connections) on the P-2812HNU-51c.

To use NAT, firewall or IGMP proxy in the P-2812HNU-51c, you need to configure a WAN connection with PPPoE or IPoE.

Note: When a layer-2 interface is in **VLAN MUX Mode** or **MSC Mode**, you can configure up to eight WAN services for each interface.

Figure 39 Internet Connection


Layer 2 Interface
Internet Connection
3G Backup
Wide Area Network (WAN) Service Setup
Choose Add, or Remove to configure a WAN service over a selected interface.
Current Mode is " ETH" WAN. Active WAN Mode is selected with the switch on the back of the device.
Interface Description Type Rate Vlan8021p VlanMuxId ConnId IGMP NAT Firewall IPv6 MLD Modify
atm0 ipoe_0_8_35 ATM/IPoE N/A N/A N/A N/A Disabled Enabled Enabled Disabled Disabled
ptm0.100 ipoe_0_0_1.100 PTM/IPoE N/A 1 100 1 Disabled Enabled Enabled Disabled Disabled
eth4.100 ipoe_eth4.100 ETH/IPoW N/A 1 100 1 Disabled Enabled Enabled Disabled Disabled
Add

The following table describes the labels in this screen.

Table 20 Internet Connection

LABEL	DESCRIPTION
Interface	This shows the name of the interface used by this connection. A default name **ipoax**, **atmx** (where x starts from 0 and is the index number of ATM layer-2 interfaces using different VPI and/or VCI values) or **ptm0** indicates the DSL port. The **pppx** name (where x starts from 1 and is the index number of PPP connection on the P-2812HNU-51c) indicates a PPP connection via any one of the WAN interface. **eth4** indicates the Ethernet WAN interface (the physical Ethernet WAN port). The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (_) represents the index number of connections through the same interface. **(null)** means the entry is not valid.
Description	This is the service name of this connection. **8** and **35** or **0** and **1** are the default VPI and VCI numbers. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection. **(null)** means the entry is not valid.
Type	This shows the layer-2 interface type and method of encapsulation used by this connection. **IPoW** stands for IPoE used in an Ethernet WAN connection.

Table 20 Internet Connection (continued)

LABEL	DESCRIPTION
Rate	This shows the maximum data rate (in Kbps) allowed for traffic sent through this connection. This displays **N/A** when there is no limit on transmission rate.
Vlan8021p	This indicates the 802.1P priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
VlanMuxId	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
ConnId	This shows the index number of each connection. This displays **N/A** when the interface used by the connection is in **Default Mode**.
IGMP	This shows whether IGMP (Internet Group Multicast Protocol) is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
NAT	This shows whether NAT is activated or not for this connection. NAT is not available when the connection uses the bridging service.
Firewall	This shows whether the firewall is activated or not for this connection. The firewall is not available when the connection uses the bridging service.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
MLD	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Remove** icon to delete the WAN connection.
Add	Click **Add** to create a new connection.

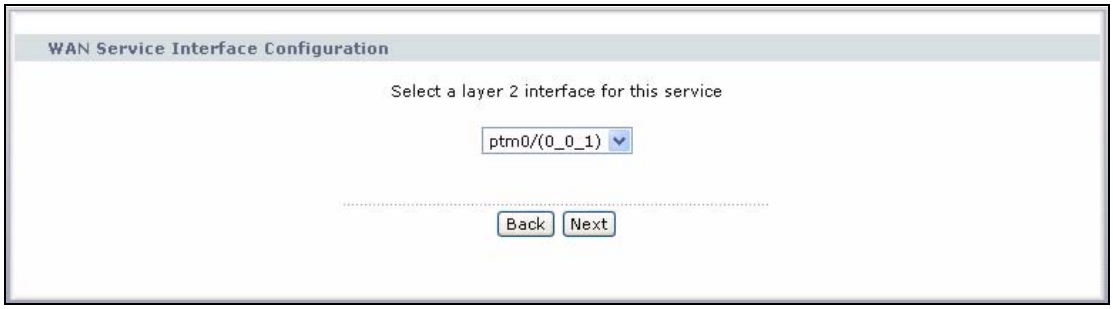
5.5.1 Internet Connection Configuration

Click the **Edit** or **Add** button in the **WAN Service** screen to configure a WAN connection.

5.5.1.1 WAN Interface

This screen displays when you add a new WAN connection.

Figure 40 WAN Configuration: WAN Interface



The following table describes the labels in this screen.

Table 21 WAN Configuration: WAN Interface

LABEL	DESCRIPTION
Select a layer 2 interface for this service	Select **ptm0** to use the DSL port as the WAN port and use the VDSL technology for data transmission. Select **atmx** or **ipoax** (where x starts from 0 and is the index number of ATM layer-2 interfaces using different VPI and/or VCI values) to use the DSL port as the WAN port and use the ADSL technology for data transmission. Select **eth4** if you want to use the Ethernet WAN port as the WAN port.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.2 Service Type

If you set the DSL link type to **PPPoA** or **IPoA** for the ATM interface and configure a WAN connection using the ATM interface, you only need to configure the **Enter Service Description** field in this screen.

Figure 41 WAN Configuration: Service Type

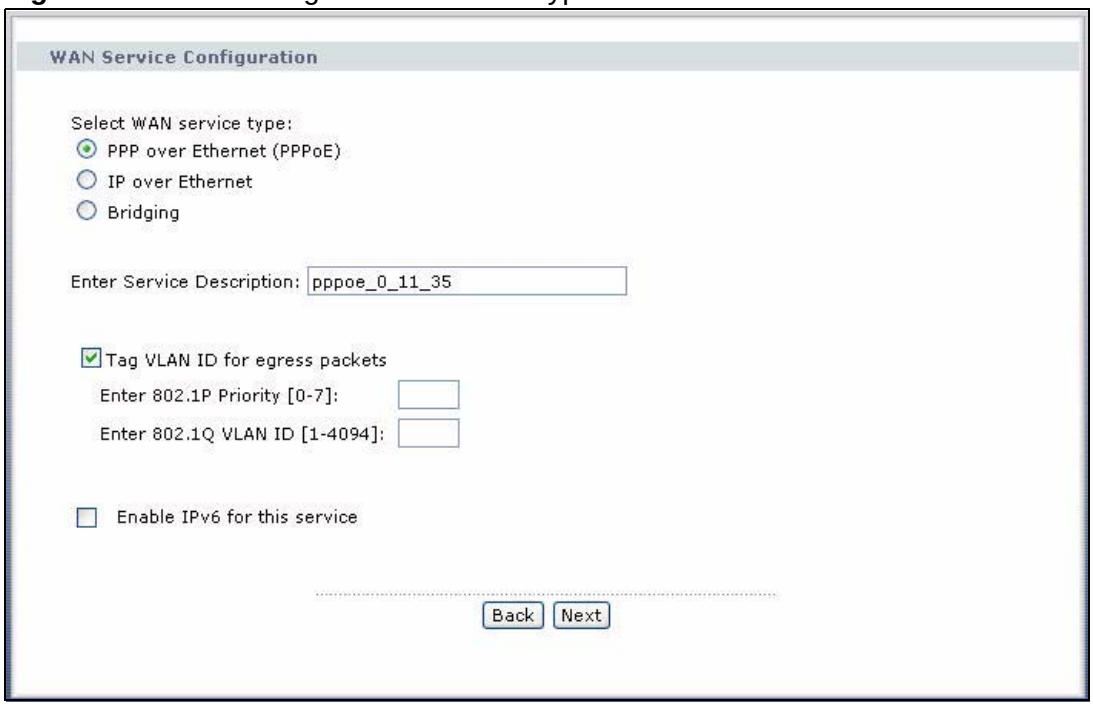
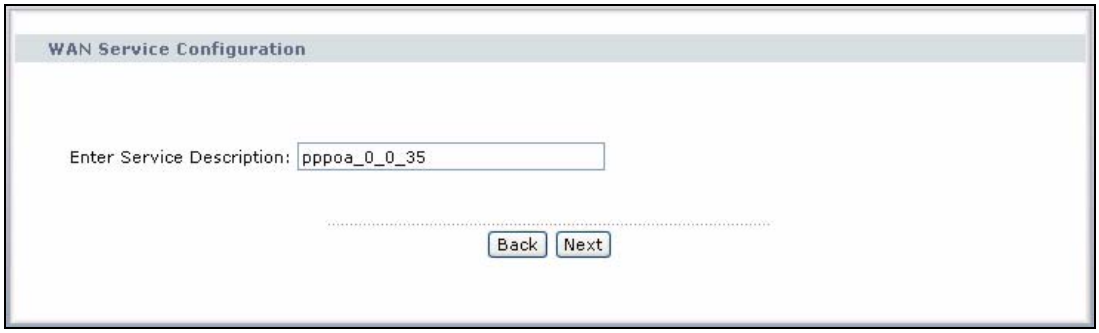


Figure 42 WAN Configuration: Service Type: PPPoA or IPoA



The following table describes the labels in this screen.

Table 22 WAN Configuration: Service Type

LABEL	DESCRIPTION
Select WAN service type	Select the method of encapsulation used by your ISP. Choices are **PPP over Ethernet (PPPoE)**, **IP over Ethernet** and **Bridging**.
Enter Service Description	Specify a name for this connection or use the automatically generated one.

Table 22 WAN Configuration: Service Type

LABEL	DESCRIPTION
Rate Limit	Enter the maximum transmission rate in Kbps for traffic sent through the WAN connection. Otherwise, leave this field blank to disable the rate limit. This field is not available for an ATM connection.
Tag VLAN ID for egress packets	Select this option to add the VLAN tag (specified below) to the outgoing traffic through this connection. This field is available when the layer-2 interface is in **VLANMUX** mode.
Enter 802.1P Priority	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. This field is available when the layer-2 interface is in **VLANMUX** mode.
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection. This field is available when the PTM interface is in **VLANMUX** mode.
Enable IPv6 for this service	Select this option to enable IPv6 for this WAN service so that the P-2812HNU-51c can use an IPv6 address when sending traffic through this connection. You can only enable IPv6 for a WAN service that uses the PPPoE or IPoE encapsulation method over the ATM or PTM interface.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

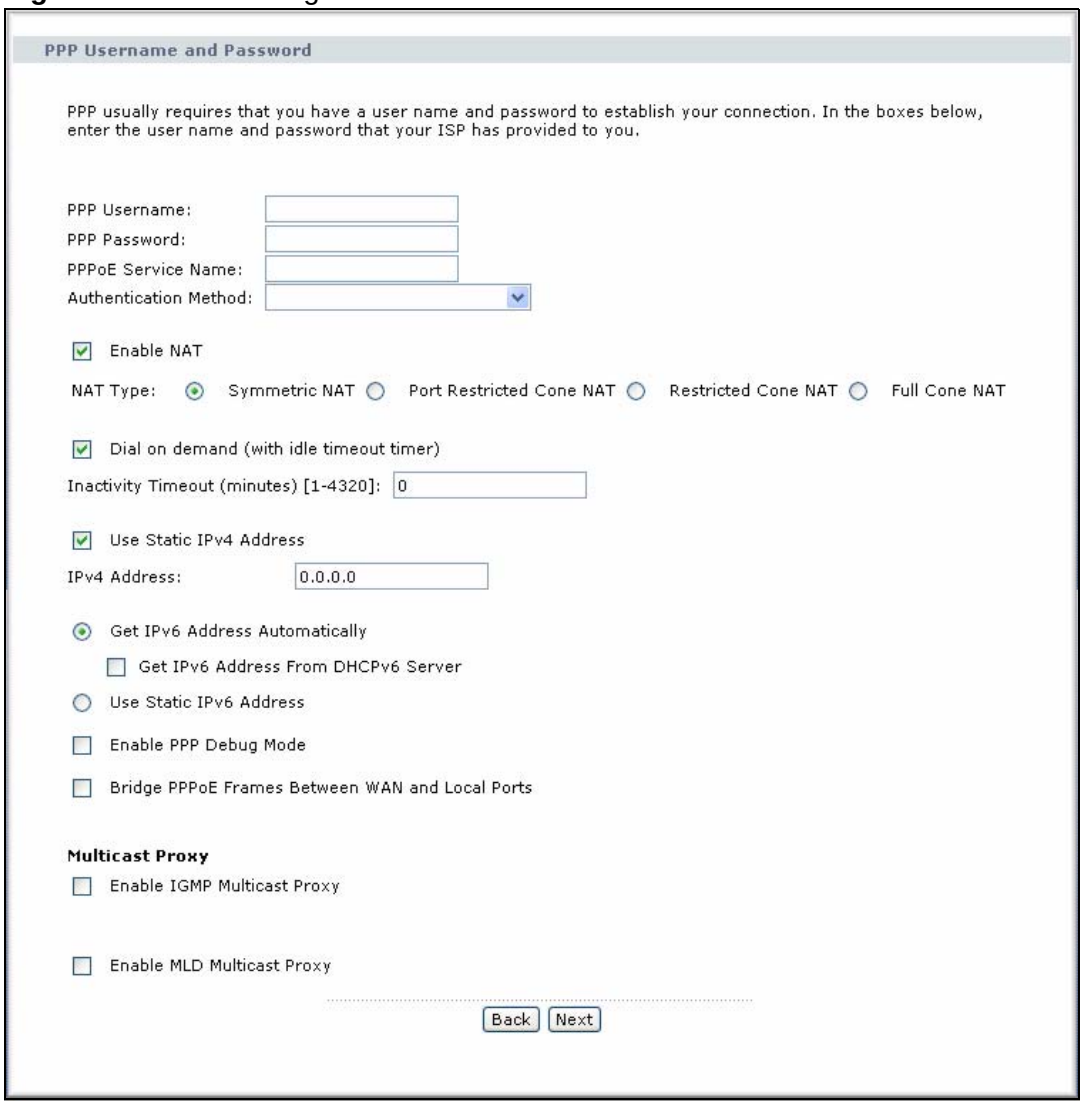
5.5.1.3 WAN IP Address and DNS Server

The screen differs by the encapsulation you selected in the previous screen. See Section 5.7 on page 125 for more information.

PPPoE or PPPoA

This screen displays when you select **PPP over Ethernet (PPPoE)** in the **WAN Service Configuration** screen or set the DSL link type to **PPPoA** for the ATM interface and configure a WAN connection using the ATM interface.

Figure 43 WAN Configuration: PPPoE


PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method:
Enable NAT
NAT Type: Symmetric NAT Port Restricted Cone NAT Restricted Cone NAT Full Cone NAT
Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]: 0
Use Static IPv4 Address
IPv4 Address: 0.0.0.0
Get IPv6 Address Automatically
Get IPv6 Address From DHCPv6 Server
Use Static IPv6 Address
Enable PPP Debug Mode
Bridge PPPoE Frames Between WAN and Local Ports
Multicast Proxy
Enable IGMP Multicast Proxy
Enable MLD Multicast Proxy
Back
Next

The following table describes the labels in this screen.

Table 23 WAN Configuration: PPPoE or PPPoA

LABEL	DESCRIPTION
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.

Table 23 WAN Configuration: PPPoE or PPPoA

LABEL	DESCRIPTION
PPPoE Service Name	Type the name of your PPPoE service here. This field is not available for a PPPoA connection.
Authentication Method	The P-2812HNU-51c supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO** - Your P-2812HNU-51c accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your P-2812HNU-51c accepts CHAP only. **PAP** - Your P-2812HNU-51c accepts PAP only. **MSCHAP** - Your P-2812HNU-51c accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.
Enable NAT	Select this option to activate NAT on this connection.
NAT Type	Select the type of NAT you want the P-2812HNU-51c to use for traffic through this connection.
Dial on Demand	Select this check box when you do not want the connection up all the time and specify an idle time-out in the **Inactivity Timeout** field.
Inactivity Timeout	Specify an idle time-out when you select **Dial on Demand**. The default setting is 0, which means the Internet session will not timeout.
Use Static IPv4 Address	A static IPv4 address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you do not have a dynamic IP address.
IPv4 Address	Enter the static IP address provided by your ISP.
Get IPv6 Address Automatically	Select this option if you want to have the P-2812HNU-51c use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Get IPv6 Address From DHCPv6 Server	Select this option if you also want to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the P-2812HNU-51c using the IPv6 prefix from an RA.
Use Static IPv6 Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the static IPv6 address provided by your ISP.
IPv6 Address Prefix Length	Enter the bit number of the IPv6 subnet mask.
Enable PPP Debug Mode	Select this option to display PPP debugging messages on the console.

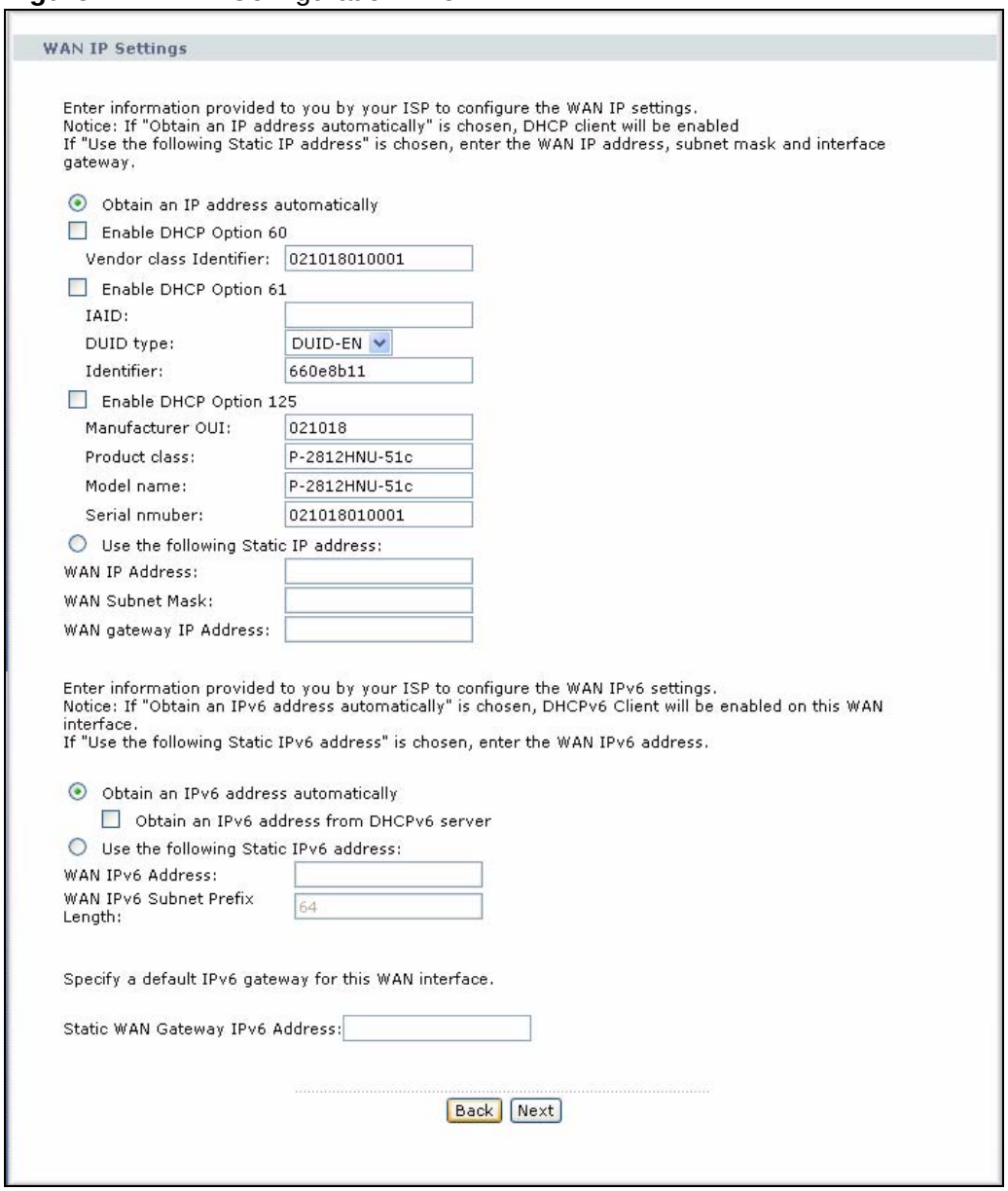
Table 23 WAN Configuration: PPPoE or PPPoA

LABEL	DESCRIPTION
Bridge PPPoE Frames Between WAN and Local Ports	Select this option to forward PPPoE packets from the WAN port to the LAN ports and from the LAN ports to the WAN port. In addition to the P-2812HNU-51c's built-in PPPoE client, you can select this to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the P-2812HNU-51c. Each host can have a separate account and a public WAN IP address. This is an alternative to NAT for application where NAT is not appropriate. Clear this if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP. This field is not available for a PPPoA connection.
Enable IGMP Multicast Proxy	Select this check box to have the P-2812HNU-51c act as an IGMP proxy on this connection. This allows the P-2812HNU-51c to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Enable MLD Multicast Proxy	Select this check box to have the P-2812HNU-51c act as an MLD proxy on this connection. This allows the P-2812HNU-51c to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoE

This screen displays when you select **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 44 WAN Configuration: IPoE


WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP client will be enabled
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.
Obtain an IP address automatically
Enable DHCP Option 60
Vendor class Identifier: 021018010001
Enable DHCP Option 61
IAID:
DUID type: DUID-EN
Identifier: 660e8b11
Enable DHCP Option 125
Manufacturer OUI: 021018
Product class: P-2812HNU-51c
Model name: P-2812HNU-51c
Serial nmuber: 021018010001
Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:
Enter information provided to you by your ISP to configure the WAN IPv6 settings.
Notice: If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.
If "Use the following Static IPv6 address" is chosen, enter the WAN IPv6 address.
Obtain an IPv6 address automatically
Obtain an IPv6 address from DHCPv6 server
Use the following Static IPv6 address:
WAN IPv6 Address:
WAN IPv6 Subnet Prefix Length: 64
Specify a default IPv6 gateway for this WAN interface.
Static WAN Gateway IPv6 Address:
Back
Next

The following table describes the labels in this screen.

Table 24 WAN Configuration: IPoE

LABEL	DESCRIPTION
Obtain an IP address automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the P-2812HNU-51c in DHCP requests that the P-2812HNU-51c sends to a DHCP server when getting a WAN IP address.
Vendor Class Identifier	Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Enable DHCP Option 61	Select this to identify the P-2812HNU-51c in DHCP requests that the P-2812HNU-51c sends to a DHCP server when getting a WAN IP address.
IAID	Enter the Identity Association Identifier (IAID) of the P-2812HNU-51c. For example, the WAN connection index number.
DUID Type	Select **Other** to enter any string that identifies the P-2812HNU-51c in the **DUID** field. Select **DUID-LL** (DUID Based on Link-layer Address) to enter the P-2812HNU-51c's hardware address, that is the MAC address in the **DUID** field. Select **DUID-EN** (DUID Assigned by Vendor Based on Enterprise Number) to enter the vendor's registered private enterprise number.
DUID	Enter the DHCP Unique Identifier (DUID) of the P-2812HNU-51c. This field is not available when you select **DUID-EN** in the **DUID Type** field.
Identifier	Enter a unique identifier assigned by the vendor. This field is available when you select **DUID-EN** in the **DUID Type** field.
Enable DHCP Option 125	Select this to add vendor specific information to DHCP requests that the P-2812HNU-51c sends to a DHCP server when getting a WAN IP address.
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Product Class	Enter the product class of the P-2812HNU-51c.
Model Name	Enter the model name of the P-2812HNU-51c.
Serial Number	Enter the serial number of the P-2812HNU-51c.
Use the following Static IP address	Select this if you have a static IP address.
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.
WAN gateway IP Address	Enter the gateway IP address provided by your ISP.

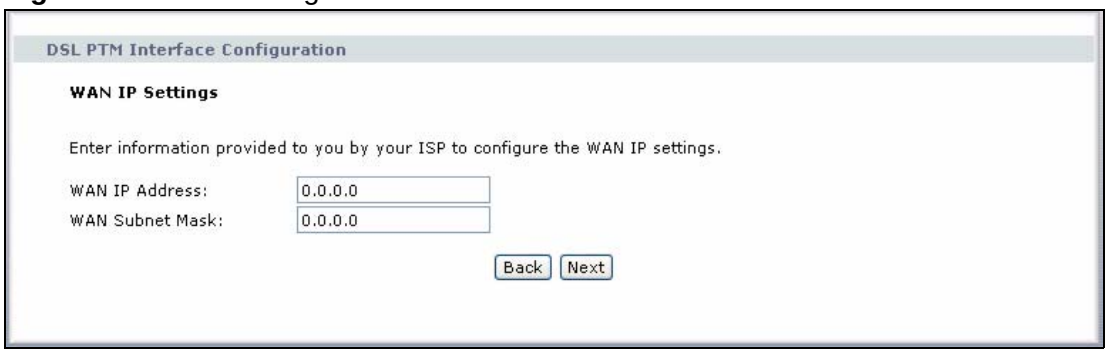
Table 24 WAN Configuration: IPoE

LABEL	DESCRIPTION
Obtain an IPv6 address automatically	Select this option if you want to have the P-2812HNU-51c use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Obtain an IPv6 address from DHCPv6 server	Select this option if you want to get an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the P-2812HNU-51c using the IPv6 prefix from an RA.
Use the following Static IPv6 address	Select this if you have a static IPv6 address.
WAN IPv6 Address	Enter the static IPv6 address provided by your ISP.
WAN IPv6 Subnet Prefix Length	Enter the bit number of the IPv6 subnet mask provided by your ISP.
Static WAN Gateway IPv6 Address	Enter the gateway IPv6 address provided by your ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoA

This screen displays only when you set the DSL link type to **IPoA** for the ATM interface and configure a WAN connection using the ATM interface.

Figure 45 WAN Configuration: IPoA



The following table describes the labels in this screen.

Table 25 WAN Configuration: IPoA

LABEL	DESCRIPTION
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.

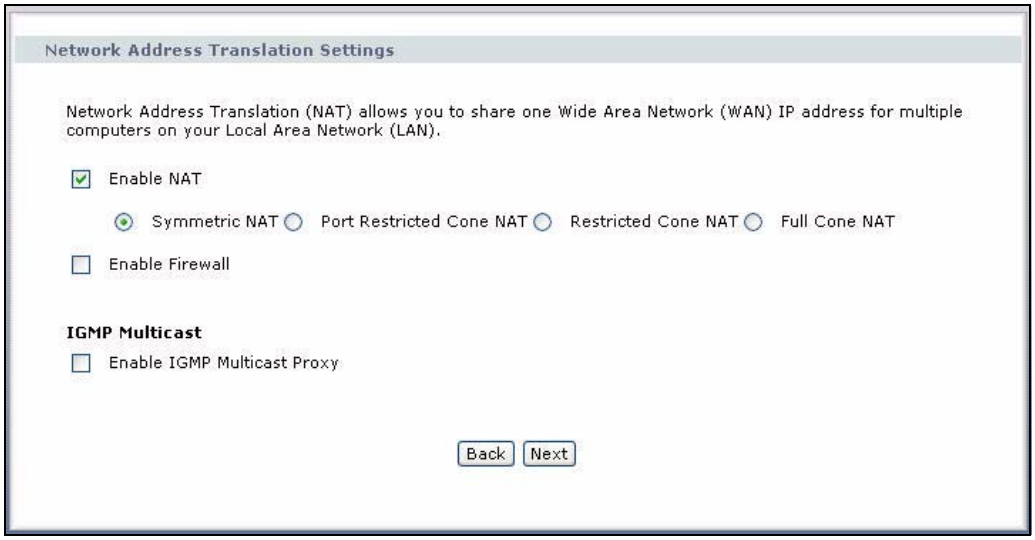
Table 25 WAN Configuration: IPoA

LABEL	DESCRIPTION
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.4 NAT, IGMP Multicast and Firewall Activation

The screen is available only when you select **IP over Ethernet** in the **WAN Service Configuration** screen or set the DSL link type to **IPoA** for the ATM interface and configure a WAN connection using the ATM interface.

Figure 46 WAN Configuration: NAT, IGMP Multicast and Firewall Activation: IPoE/ IPoA


Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Symmetric NAT
Port Restricted Cone NAT
Restricted Cone NAT
Full Cone NAT
Enable Firewall
IGMP Multicast
Enable IGMP Multicast Proxy
Back
Next

The following table describes the labels in this screen.

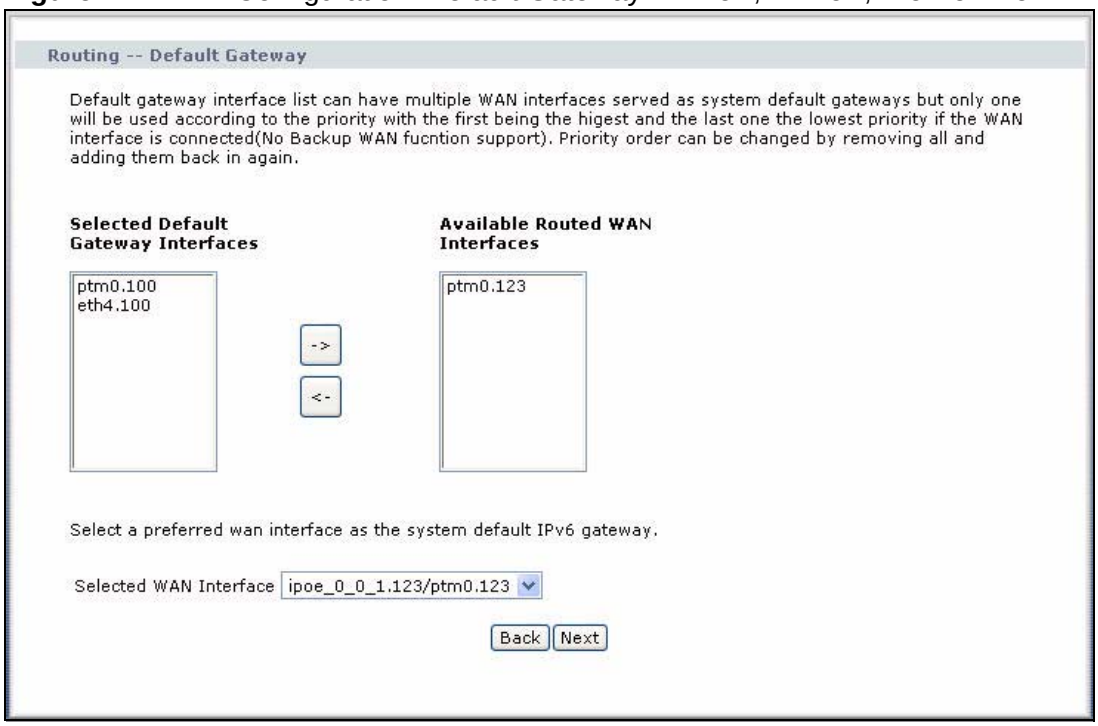
Table 26 WAN Configuration: NAT, IGMP Multicast and Firewall Activation: IPoE

LABEL	DESCRIPTION
Enable NAT	Select this option to activate NAT on this connection.
	Select the type of NAT you want the P-2812HNU-51c to use for traffic through this connection.
Enable Firewall	Select this check box to activate Firewall on this connection.
Enable IGMP Multicast Proxy	Select this check box to have the P-2812HNU-51c act as an IGMP proxy on this connection. This allows the P-2812HNU-51c to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.5 Default Gateway

The screen is not available when you select **Bridging** in the **WAN Service Configuration** screen.

Figure 47 WAN Configuration: Default Gateway: PPPoE, PPPoA, IPoE or IPoA


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected(No Backup WAN fucntion support). Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ptm0.100
eth4.100
->
<-
ptm0.123
Select a preferred wan interface as the system default IPv6 gateway.
Selected WAN Interface
ipoe_0_0_1.123/ptm0.123
Back
Next

The following table describes the labels in this screen.

Table 27 WAN Configuration: Default Gateway: PPPoE, PPPoA, IPoE or IPoA

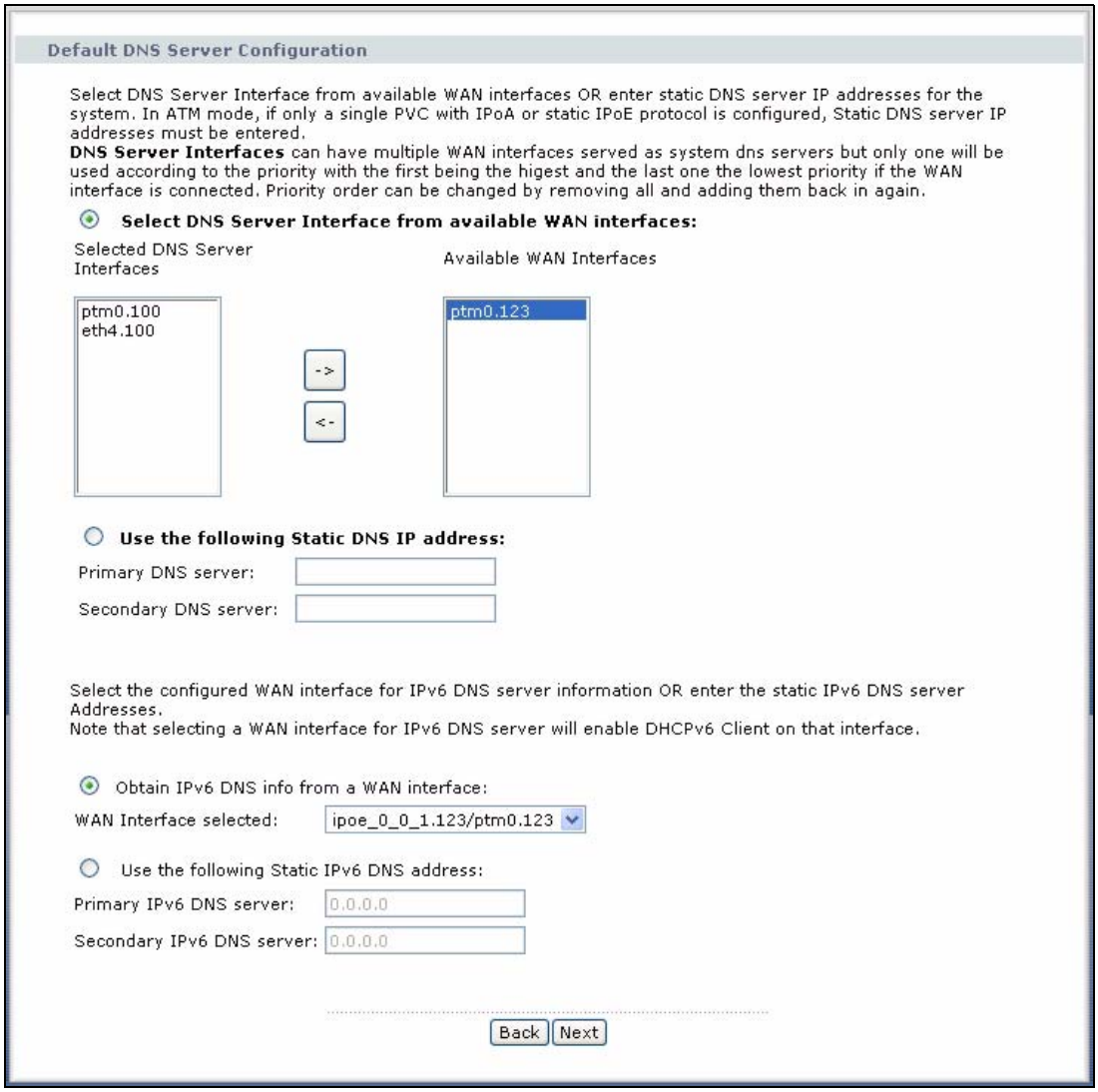
LABEL	DESCRIPTION
Selected Default Gateway Interfaces Available Routed WAN Interfaces	Select a WAN interface through which you want to forward the traffic. Select a WAN interface in the **Available Routed WAN Interfaces** box and use the left-facing arrow to move it to the **Selected Default Gateway Interfaces** box to use that interface as the default gateway. To remove a WAN interface from the **Selected Default Gateway Interfaces** box, use the righ-facing arrow. The interface on the top of the list gets the highest priority.
Selected WAN Interface	Select a WAN interface to use that interface as the system default IPv6 gateway. This field is available only when you configure a WAN service with IPv6 enabled. You can only enable IPv6 for a WAN service that uses the PPPoE or IPoE encapsulation method over the ATM or PTM interface.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.6 DNS Server

The screen is not available when you select **Bridging** in the **WAN Service Configuration** screen.

Note: If you configure only one IPoA or IPoE connection using the ATM interface on the P-2812HNU-51c, you must enter the static DNS server address.

Figure 48 WAN Configuration: DNS Server: PPPoE, PPPoA, IPoE or IPoA


Default DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
ptm0.100
eth4.100
->
<-
ptm0.123
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.
Obtain IPv6 DNS info from a WAN interface:
WAN Interface selected:
ipoe_0_0_1.123/ptm0.123
Use the following Static IPv6 DNS address:
Primary IPv6 DNS server:
0.0.0.0
Secondary IPv6 DNS server:
0.0.0.0
Back
Next

The following table describes the labels in this screen.

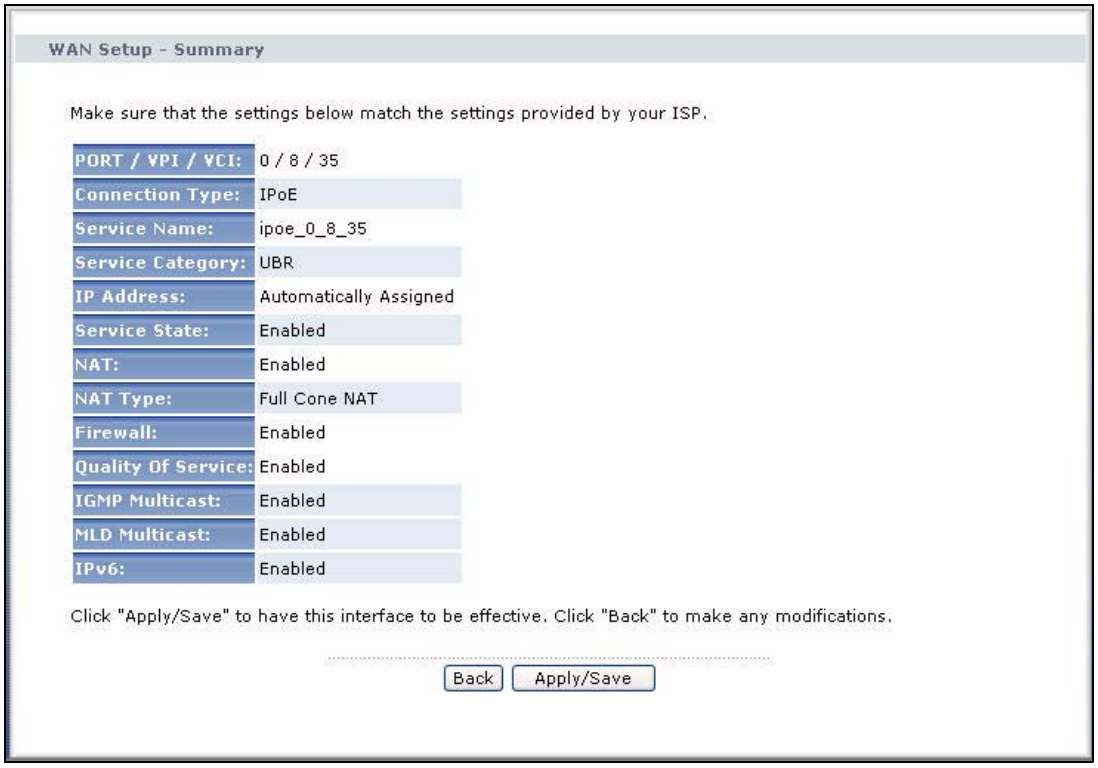
Table 28 WAN Configuration: DNS Server: PPPoE, PPPoA, IPoE or IPoA

LABEL	DESCRIPTION
Select DNS Server Interface from available WAN interfaces	Select this to have the P-2812HNU-51c get the DNS server addresses from the ISP automatically.
Selected DNS Server Interfaces Available WAN Interfaces	Select a WAN interface through which you want to obtain the DNS related information. Select a WAN interface in the **Available WAN Interfaces** box and use the left-facing arrow to move it to the **Selected DNS Server Interfaces** box to use that interface as the DNS server. To remove a WAN interface from the **Selected DNS Server Interfaces** box, use the righ-facing arrow. The interface on the top of the list gets the highest priority.
Use the following Static DNS IP address	Select this to have the P-2812HNU-51c use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
	The following fields are available only when you configure a WAN service with IPv6 enabled. You can only enable IPv6 for a WAN service that uses the PPPoE or IPoE encapsulation method over the ATM or PTM interface.
Obtain IPv6 DNS info from a WAN interface	Select this to have the P-2812HNU-51c get the IPv6 DNS server addresses from the ISP automatically.
WAN Interface selected	Select a WAN interface through which you want to obtain the IPv6 DNS related information.
Use the following Static IPv6 DNS address	Select this to have the P-2812HNU-51c use the IPv6 DNS server addresses you configure manually.
Primary IPv6 DNS server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary IPv6 DNS server	Enter the second IPv6 DNS server address assigned by the ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.7 Configuration Summary

This read-only screen shows the current WAN connection settings.

Figure 49 WAN Configuration: Configuration Summary


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
PORT / VPI / VCI: 0 / 8 / 35
Connection Type: IPoE
Service Name: ipoe_0_8_35
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Enabled
NAT Type: Full Cone NAT
Firewall: Enabled
Quality Of Service: Enabled
IGMP Multicast: Enabled
MLD Multicast: Enabled
IPv6: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

The following table describes the labels in this screen.

Table 29 WAN Configuration: Configuration Summary

LABEL	DESCRIPTION
Port / VPI / VCI	This is the DSL port number, VPI and VCI for an ATM connection. This displays **N / A** for an Ethernet WAN conenction or not available for a PTM connection.
Connection Type	This is the encapsulation method used by this connection.
Service Name	This is the name of the service.
Service Category	This is the ATM traffic class. This field is blank for a PTM or Ethernet WAN conenction.
IP Address	This shows whether the WAN IP address is assigned by the ISP, manually configured or not configurable.
Service State	This shows whether this service is active or not.
NAT	This shows whether NAT is active or not for this connection.
NAT Type	This shows the type of NAT the P-2812HNU-51c uses on this connection.
Firewall	This shows whether Firewall is active or not for this connection.

Table 29 WAN Configuration: Configuration Summary

LABEL	DESCRIPTION
Quality Of Service	This shows whether QoS is active or not for this connection.
IGMP Multicast	This shows whether IGMP multicasting is active or not for this connection.
MLD Multicast	This shows whether MLD multicasting is active or not for this connection.
IPv6	This shows whether IPv6 is active or not for this connection.
Back	Click this button to return to the previous screen.
Apply/Save	Click this button to save your changes.

5.6 The 3G Backup Screen

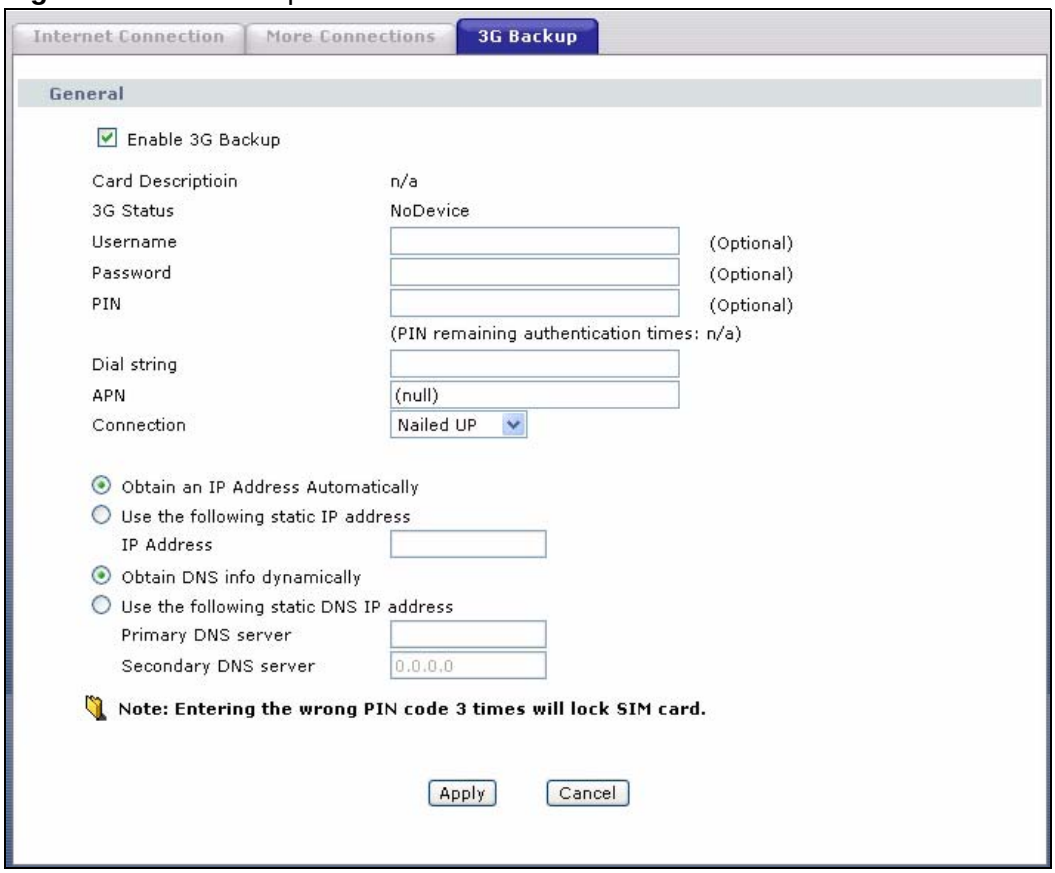
Use this screen to configure your 3G settings. Click **Network > WAN > 3G Backup**.

At the time of writing, the 3G cards you can use in the P-2812HNU-51c are Huawei E220, Huawei E169U, and Qisda H21.

Note: The actual data rate you obtain varies depending the 3G card you use, the signal strength to the service provider's base station, and so on.

If the signal strength of a 3G network is too low, the 3G card may switch to an available 2.5G or 2.75G network. Refer to Section 5.7 on page 125 for a comparison between 2G, 2.5G, 2.75G and 3G wireless technologies.

Figure 50 3G Backup



The following table describes the labels in this screen.

Table 30 3G Backup

LABEL	DESCRIPTION
Enable 3G Backup	Select this option to have the P-2812HNU-51c use the 3G connection as your WAN or a backup when the wired WAN connection fails.
Card Descriptioin	This field displays the manufacturer and model name of your 3G card if you inserted one in the P-2812HNU-51c. Otherwise, it displays **n/a**.

Table 30 3G Backup (continued)

LABEL	DESCRIPTION
3G Status	This field displays: • **NoDevice** when no 3G card is inserted, • **Disabled** when the 3G WAN is not activated, • **Up** when the 3G WAN connection is up, • **Down** when the 3G connection is down, • **NoResponse** when there is no response from the inserted 3G card, • **NeedPIN** if the PIN code you entered in the **PIN** field is not the right one for the 3G card you inserted, • **NeedPUK** if you enter the PIN (Personal Identification Number) code incorrectly for three times and the SIM card is blocked by your ISP, or • **DamagedSIM** when the SIM card is damaged or not inserted. If a link displays in this field, click the link to view more status information or enter the correct PIN or PUK (Personal Unblocking Key) code.
User Name	Type the user name (of up to 70 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 70 ASCII printable characters) associated with the user name above.
PIN	A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card. If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, leave this field blank.
Dial string	Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number. For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan.
APN	Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 31 ASCII printable characters. Spaces are allowed.
Connection	Select **Nailed Up** if you do not want the connection to time out. Select **on Demand** if you do not want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	This value specifies the time in minutes that elapses before the P-2812HNU-51c automatically disconnects from the ISP. **0** means the Internet session will not timeout.

Table 30 3G Backup (continued)

LABEL	DESCRIPTION
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address.
Use the following static IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use the following static IP address**.
Obtain DNS info dynamically	Select this to have the P-2812HNU-51c get the DNS server addresses from the ISP automatically.
Use the following static DNS IP address	Select this to have the P-2812HNU-51c use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to return to the previous configuration.

5.7 Technical Reference

The following section contains additional technical information about the P-2812HNU-51c features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The P-2812HNU-51c can work in bridge mode or routing mode. When the P-2812HNU-51c is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over Ethernet

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF

standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the P-2812HNU-51c (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-2812HNU-51c does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The P-2812HNU-51c encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

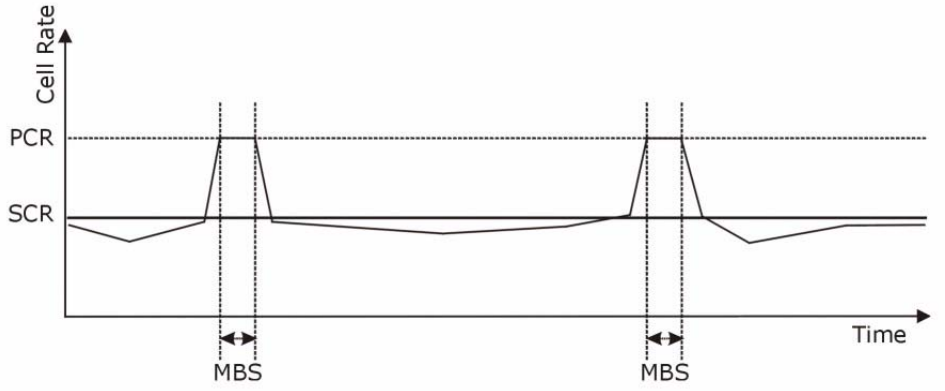
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 51 Example of Traffic Shaping



ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

IP Address Assignment

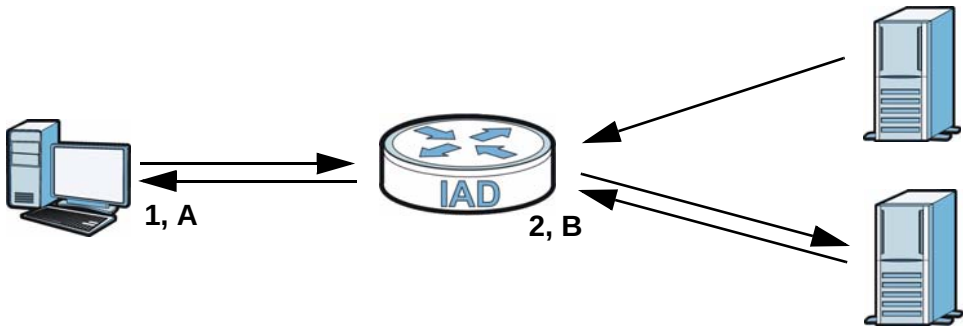
A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

Full Cone NAT

In full cone NAT, the NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The NAT router also maps packets coming to that external IP address and port to the internal IP address and port.

In the following example, the P-2812HNU-51c maps the source address of all packets sent from the internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. The P-2812HNU-51c also performs NAT on all incoming packets sent to IP address **2** and port **B** and forwards them to IP address **1**, port **A**.

Figure 52 Full Cone NAT Example



Restricted Cone NAT

As in full cone NAT, a restricted cone NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the NAT router maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network.

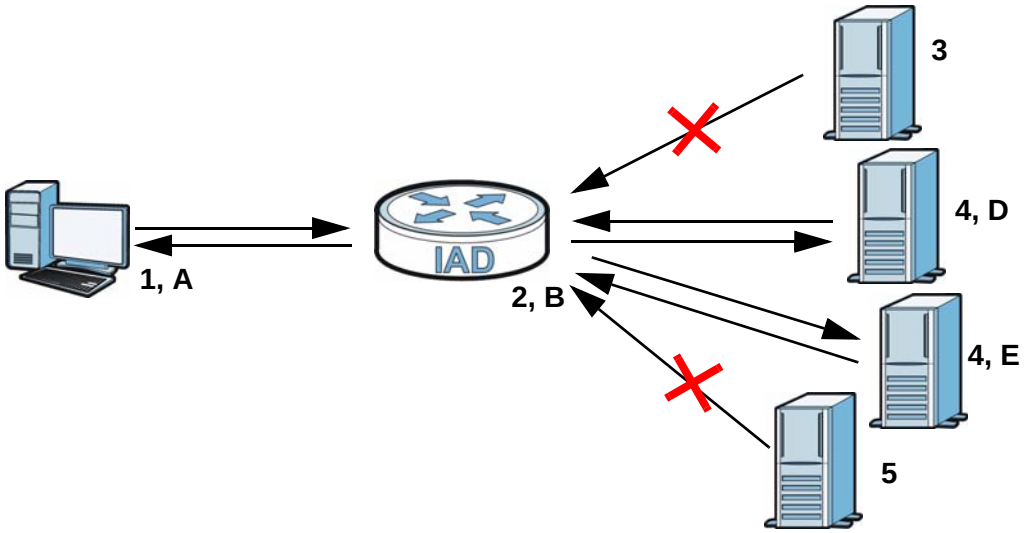
The difference from full cone NAT is in how the restricted cone NAT router handles packets coming in from the external network. A host on the external network (IP address **3** or IP address **4** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address.

A server with IP address **1** and port **A** sends packets to IP address **4**. The P-2812HNU-51c changes the server's IP address to **2** and port to **B**.

Both **4, D** and **4, E** can send packets to **2**, **B** since **1**, **A** has already sent packets to **4**. The P-2812HNU-51c will perform NAT on the packets from **4, D** and **4, E** and

send them to the server at IP address **1**, port **A**. Packets have not been sent from **1**, **A** to **3** or **5**, so **3** and **5** cannot send packets to **1**, **A**.

Figure 53 Restricted Cone NAT Example



Port Restricted Cone NAT

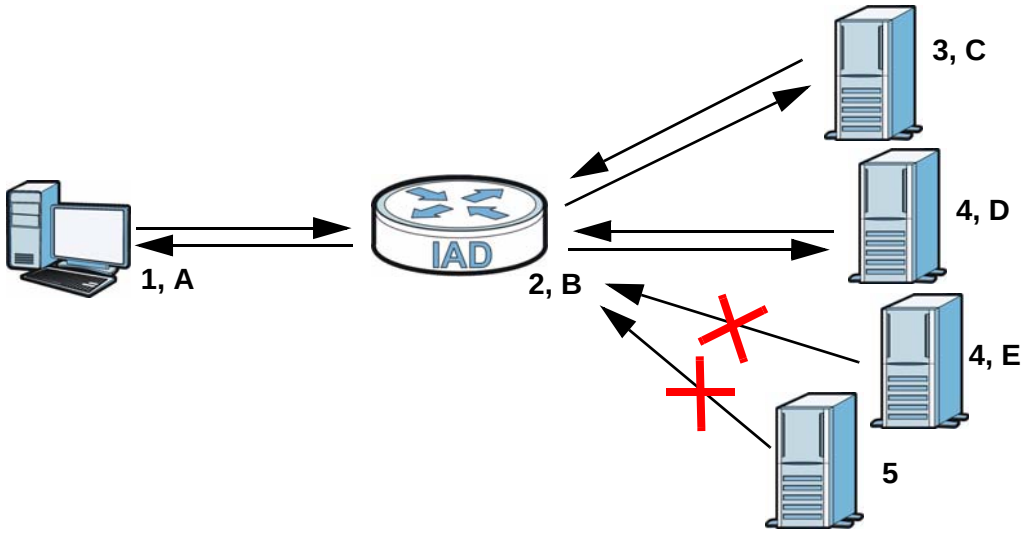
Port restricted cone NAT maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the P-2812HNU-51c maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. A host on the external network (IP address **3** and Port **C** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address and port.

A server with IP address **1** and port **A** sends packets to IP address **3**, port **C** and IP address **4**, port **D**. The P-2812HNU-51c changes the server's IP address to **2** and port to **B**.

Since **1**, **A** has already sent packets to **3**, **C** and **4**, **D,** they can send packets back to **2**, **B** and the P-2812HNU-51c will perform NAT on them and send them to the server at IP address **1**, port **A**.

Packets have not been sent from **1**, **A** to **4**, **E** or **5**, so they cannot send packets to **1**, **A**.

Figure 54 Port Restricted Cone NAT Example



Symmetric NAT

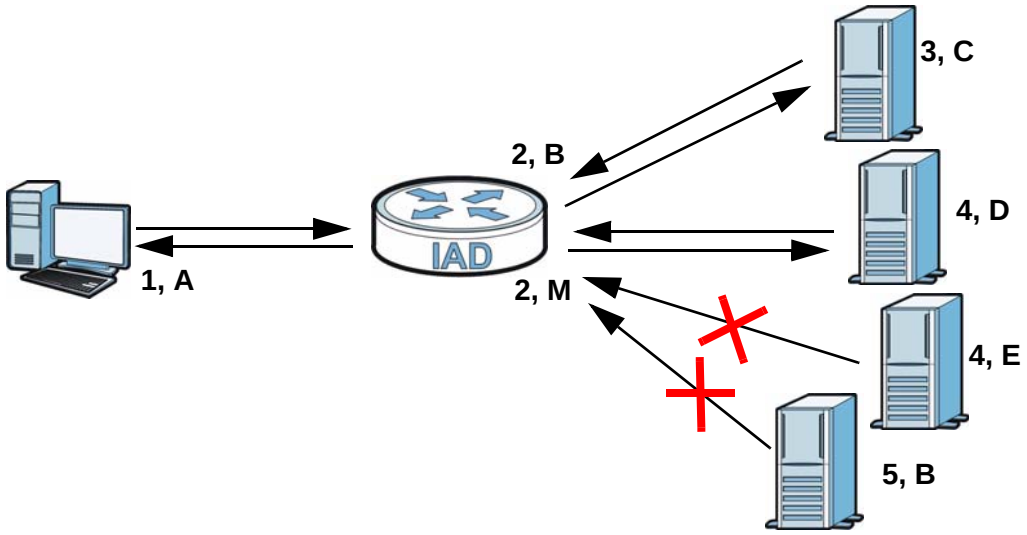
The full, restricted and port restricted cone NAT types use the same mapping for an outgoing packet's source address regardless of the destination IP address and port. In symmetric NAT, the mapping of an outgoing packet's source address to a source address in another network is different for each different destination IP address and port.

In the following example, the P-2812HNU-51c maps the source address IP address **1** and port **A** to IP address **2** and port **B** on the external network for packets sent to IP address **3** and port **C**. The P-2812HNU-51c uses a different mapping (IP address **2** and port **M**) for packets sent to IP address **4** and port **D**.

A host on the external network (IP address **3** and port **C** for example) can only send packets to the internal host via the external IP address and port that the NAT router used in sending a packet to the external host's IP address and port. So in

the example, only **3, C** is allowed to send packets to **2, B** and only **4, D** is allowed to send packets to **2, M**.

Figure 55 Symmetric NAT



Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and

contains two bytes of TPID (Tag Protocol Identifier), residing within the type/ length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the P-2812HNU-51c queries all directly connected networks to gather group membership. After that, the P-2812HNU-51c periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is

204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The P-2812HNU-51c can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2 If your ISP dynamically assigns the DNS server IP addresses (along with the P-2812HNU-51c's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

3G Comparison Table

See the following table for a comparison between 2G, 2.5G, 2.75G and 3G wireless technologies.

Table 31 2G, 2.5G, 2.75G, 3G and 3.5G Wireless Technologies

NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	CDMA-BASED	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	Slow ↓ Fast
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio. CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.		
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU[A] specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		

A. The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.

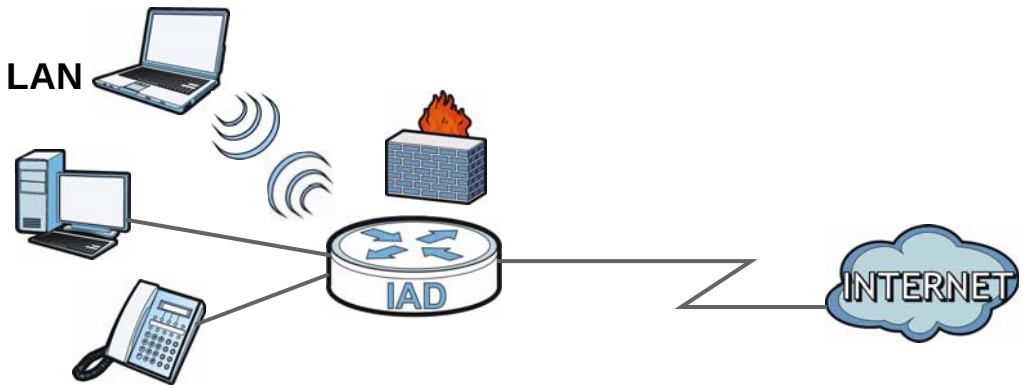
6

LAN Setup

6.1 Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.



- See Section 6.5 on page 143 for more information on LANs.
- See Appendix E on page 467 for more information on IP addresses and subnetting.

6.1.1 What You Can Do in this Chapter

- The **IP** screen lets you set the LAN IPv4 address and subnet mask of your P-2812HNU-51c and configure other LAN TCP/IP settings (Section 6.4 on page 142).
- The **IPv6** screen lets you set the IPv6 settings for your P-2812HNU-51c LAN interface (Section 6.4 on page 142).

6.2 What You Need To Know

IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your P-2812HNU-51c will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-2812HNU-51c unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This P-2812HNU-51c has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DHCP Relay

You can also configure the P-2812HNU-51c to relay client DHCP requests to a DHCP server and the server’s responses back to the clients.

RIP

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.

Multicast and IGMP

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are two versions 1 and 2. IGMP version 2 is an improvement over version 1 but IGMP version 1 is still in wide use.

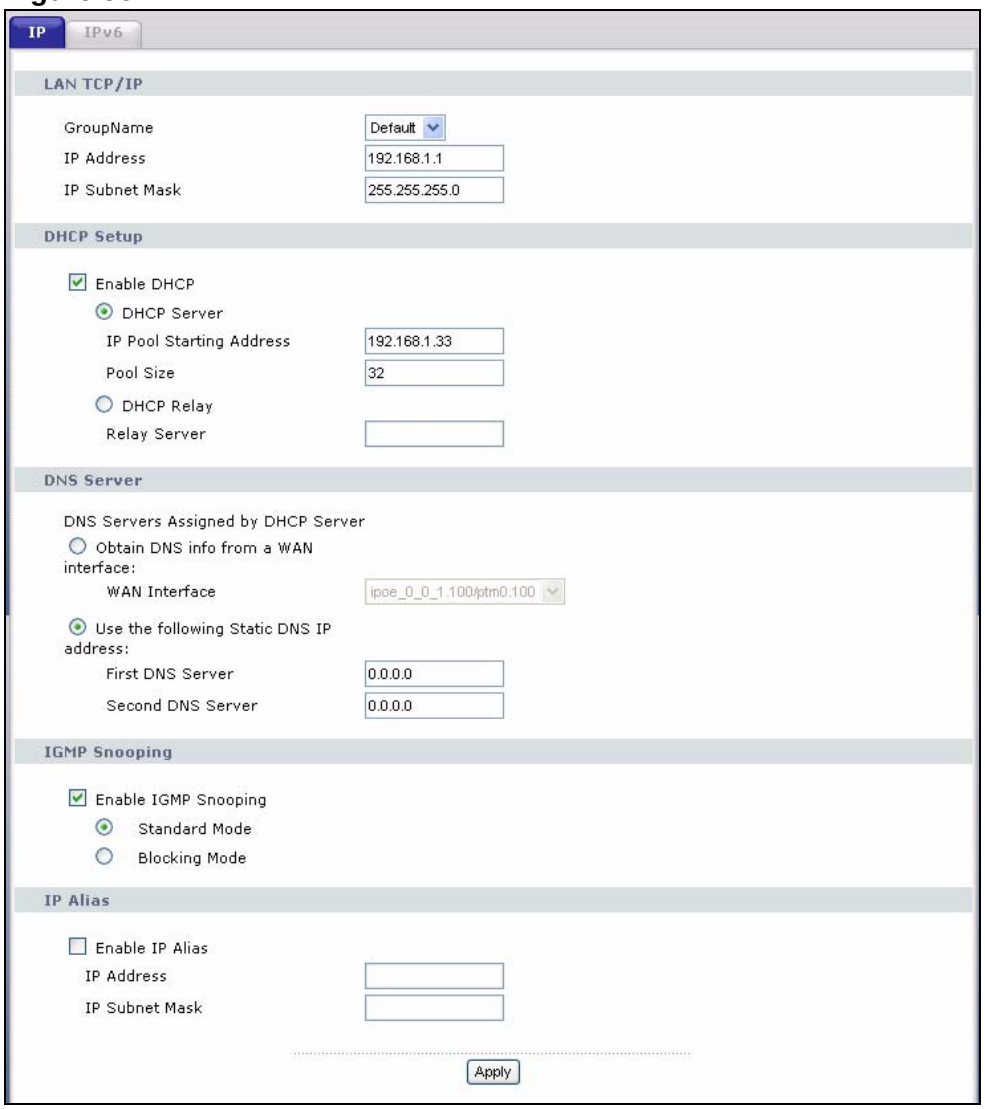
DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

6.3 The LAN IP Screen

Click **Network > LAN** to open the **IP** screen. See Section 6.5 on page 143 for background information. Use this screen to set the Local Area Network IPv4 address and subnet mask of your P-2812HNU-51c.

Figure 56 LAN > IP



The following table describes the fields in this screen.

Table 32 LAN > IP

LABEL	DESCRIPTION
LAN TCP/IP	
Group Name	Select the interface group for which you want to configure the LAN TCP/IP settings. See Chapter 13 on page 117 for how to create a new interface group.
IP Address	Enter the LAN IPv4 address you want to assign to your P-2812HNU-51c in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
DHCP Setup	
Active DHCP	Select this to have the P-2812HNU-51c act as a DHCP server or DHCP relay agent. Otherwise, deselect this to not have the P-2812HNU-51c provide any DHCP services. The DHCP server will be disabled.
DHCP Server	Select this option to have the P-2812HNU-51c assign IP addresses and provide subnet mask, gateway, and DNS server information to the network. The P-2812HNU-51c is the DHCP server for the network. When the P-2812HNU-51c acts as a DHCP server, the following items need to be set:
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Relay	Select this option to have the P-2812HNU-51c forward DHCP request to the DHCP server.
Relay Server	If you select **DHCP Relay**, enter the IP address of the DHCP server.
DNS Servers Assigned by DHCP Server The P-2812HNU-51c passes DNS (Domain Name System) server addresses to the LAN DHCP clients. If you do not configure DNS servers, the P-2812HNU-51c uses its LAN IP address and tells the DHCP clients on the LAN that itself is the DNS server. When a LAN client sends a DNS query to the P-2812HNU-51c, the P-2812HNU-51c forwards the query to its system DNS server you configured in the WAN screen.	
Obtain DNS info from a WAN interface	Select this if your ISP dynamically assigns DNS server information.
WAN Interfaces	Select a WAN interface through which you obtain the DNS related information.
Use the following Static DNS IP address	Select this if you want to configure the DNS server addresses manually.
First DNS Server	Enter the first DNS server IP address the P-2812HNU-51c passes to the DHCP clients.

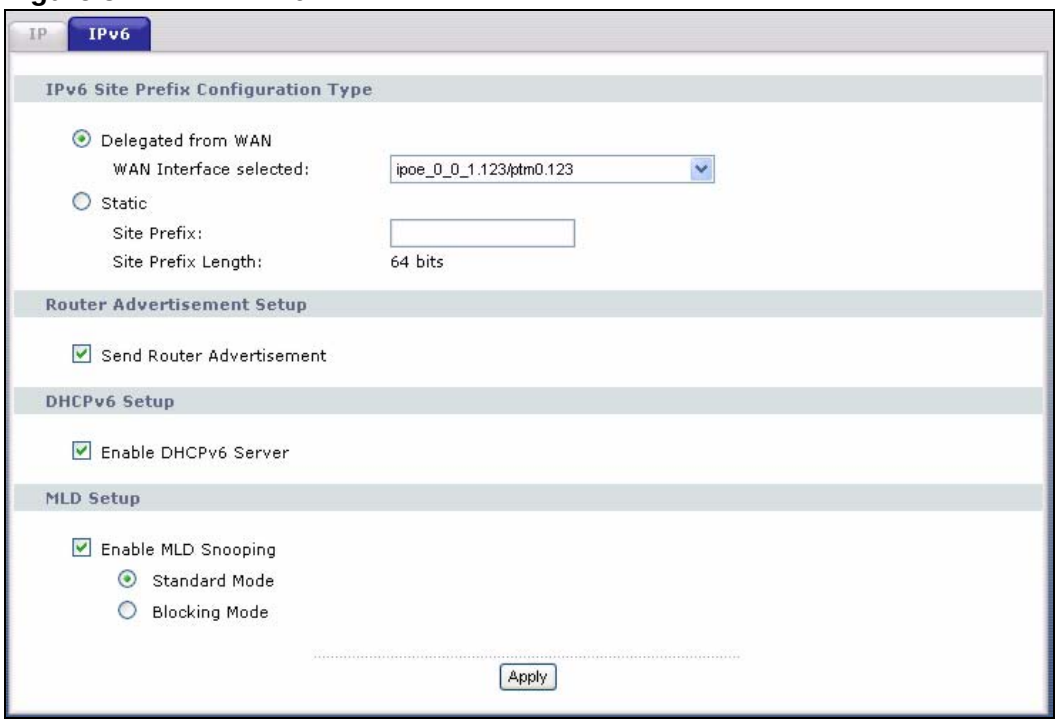
Table 32 LAN > IP

LABEL	DESCRIPTION
Second DNS Server	Enter the second DNS server IP address the P-2812HNU-51c passes to the DHCP clients.
IGMP Snooping	
Enable IGMP Snooping	Select this option to activate IGMP snooping. This allows the P-2812HNU-51c to passively learn multicast group.
Standard Mode	Select this to have the P-2812HNU-51c forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports.
Blocking Mode	Select this to have the P-2812HNU-51c block all unknown multicast packets from the WAN.
Enable IP Alias	Select the check box to configure another LAN network for the P-2812HNU-51c.
IP Address	Enter the IP address of your P-2812HNU-51c in dotted decimal notation.
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.

6.4 The LAN IPv6 Screen

Click **Network > LAN > IPv6** to open the **IPv6** screen. See Section 5.7 on page 125 for background information about IPv6. Use this screen to configure the IPv6 settings for your P-2812HNU-51c's LAN interface.

Figure 57 LAN > IPv6



The following table describes the fields in this screen.

Table 33 LAN > IPv6

LABEL	DESCRIPTION
IPv6 Site Prefix Configuration Type	Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. The P-2812HNU-51c uses the prefix to generate an IPv6 address.
Delegated from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
WAN Interface selected	Select a WAN interface through which you want to get an IPv6 network prefix. You should already have configured a WAN service with IPv6 enabled.
Static	Select this option to configure a fixed IPv6 network prefix for the P-2812HNU-51c's LAN interface.
Site Prefix	Enter the IPv6 prefix that the P-2812HNU-51c uses to generate its LAN IPv6 address.
Site Prefix Length	An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.

Table 33 LAN > IPv6

LABEL	DESCRIPTION
Router Advertisement Setup	Router advertisement is a response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters, such as IPv6 prefix and DNS information. Router solicitation is a request from a host to locate a router that can act as the default router and forward packets.
Send Router Advertisement	Select this option to have the P-2812HNU-51c send router advertisement messages to the LAN hosts. Note: The LAN hosts neither generate global IPv6 addresses nor communicate with other networks if you disable this feature.
DHCPv6 Setup	
Enable DHCPv6 Server	Select this option to have the P-2812HNU-51c act as a DHCP server to assign and pass IPv6 network addresses, prefixes and DNS server information to its DHCP clients.
MLD Setup	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
Enable MLD Snooping	Select this option to activate MLD snooping on the P-2812HNU-51c. This allows the P-2812HNU-51c to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.

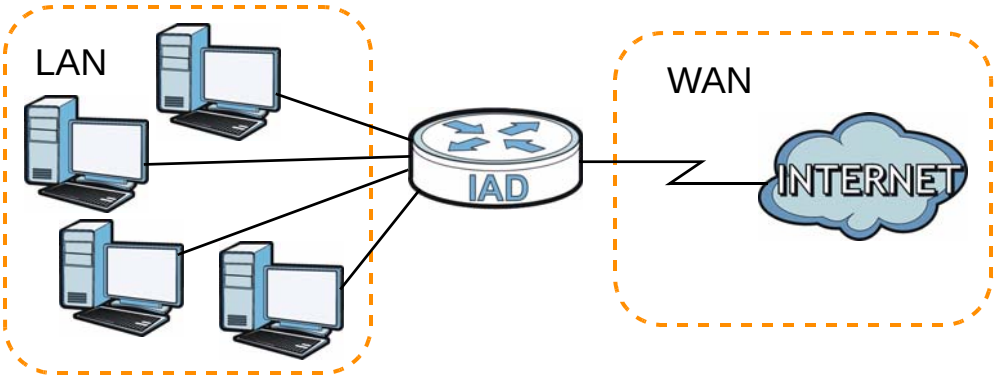
6.5 Technical Reference

The following section contains additional technical information about the P-2812HNU-51c features described in this chapter.

LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the P-2812HNU-51c ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 58 LAN and WAN IP Addresses



DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the P-2812HNU-51c as a DHCP server or disable it. When configured as a server, the P-2812HNU-51c provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The P-2812HNU-51c is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

LAN TCP/IP

The P-2812HNU-51c has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP

addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the P-2812HNU-51c. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your P-2812HNU-51c, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your P-2812HNU-51c will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-2812HNU-51c unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The P-2812HNU-51c supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the P-2812HNU-51c queries all directly connected networks to gather group membership. After that, the P-2812HNU-51c periodically updates this information. IP multicasting can be enabled/disabled on the P-2812HNU-51c LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

IP Alias

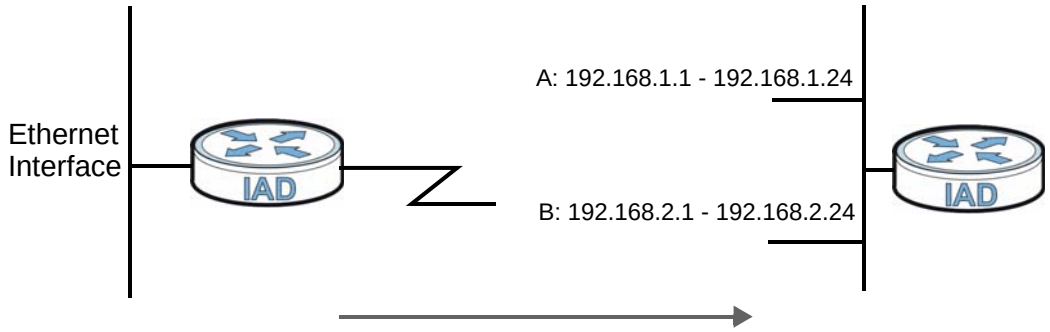
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The P-2812HNU-51c supports three logical LAN interfaces via its single physical Ethernet interface with the P-2812HNU-51c itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Note: Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A and B.

Figure 59 Physical Network & Partitioned Logical Networks



7

Wireless LAN

7.1 Overview

This chapter describes how to perform tasks related to setting up and optimizing your wireless network, including the following.

- Turning the wireless connection on or off.
- Configuring a name, wireless channel and security for the network.
- Using WiFi Protected Setup (WPS) to configure your wireless network.
- Using a MAC (Media Access Control) address filter to restrict access to the wireless network.

See Chapter 2 on page 33 for a tutorial showing how to set up your wireless connection in an example scenario.

See Section 7.11 on page 171 for advanced technical information on wireless networks.

7.1.1 What You Can Do in this Chapter

This chapter describes the P-2812HNU-51c's **Network > Wireless LAN** screens. Use these screens to set up your P-2812HNU-51c's wireless connection.

- The **General** screen lets you turn the wireless connection on or off, set up wireless security and make other basic configuration changes (Section 7.4 on page 153). You can also configure the MAC filter to allow or block access to the P-2812HNU-51c based on the MAC addresses of the wireless stations.
- The **More AP** screen lets you set up multiple wireless networks on your P-2812HNU-51c (Section 7.5 on page 162).
- Use the **WPS** screen and the **WPS Station** screen to use WiFi Protected Setup (WPS). WPS lets you set up a secure network quickly, when connecting to other WPS-enabled devices.

  Use the **WPS** screen (see Section 7.6 on page 163) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the P-2812HNU-51c's WPS status.

  Use the **WPS Station** (see Section 7.7 on page 165) screen to set up WPS by pressing a button or using a PIN.

- The **WDS** screen lets you set up a Wireless Distribution System, in which the P-2812HNU-51c acts as a bridge with other ZyXEL access points (Section 7.8 on page 166).
- The **Scheduling** screen lets you set the times your wireless LAN is turned off (Section 7.9 on page 167).
- The **Advanced Setup** screen lets you change the wireless mode, and make other advanced wireless configuration changes (Section 7.10 on page 170).

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and some security in the **General** screen.

7.2 What You Need to Know

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Wireless Network Construction

Wireless networks consist of wireless clients, access points and bridges.

- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

Network Names

Each network must have a name, referred to as the SSID - “Service Set IDentifier”. The “service set” is the network, so the “service set identifier” is the network’s name. This helps you identify your wireless network when wireless networks’ coverage areas overlap and you have a variety of networks to choose from.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

Wireless Security

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network she/he can either steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a “key” phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is perfectly secure if you use a long key which is difficult for an attacker’s software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See Section 7.2 on page 150 if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

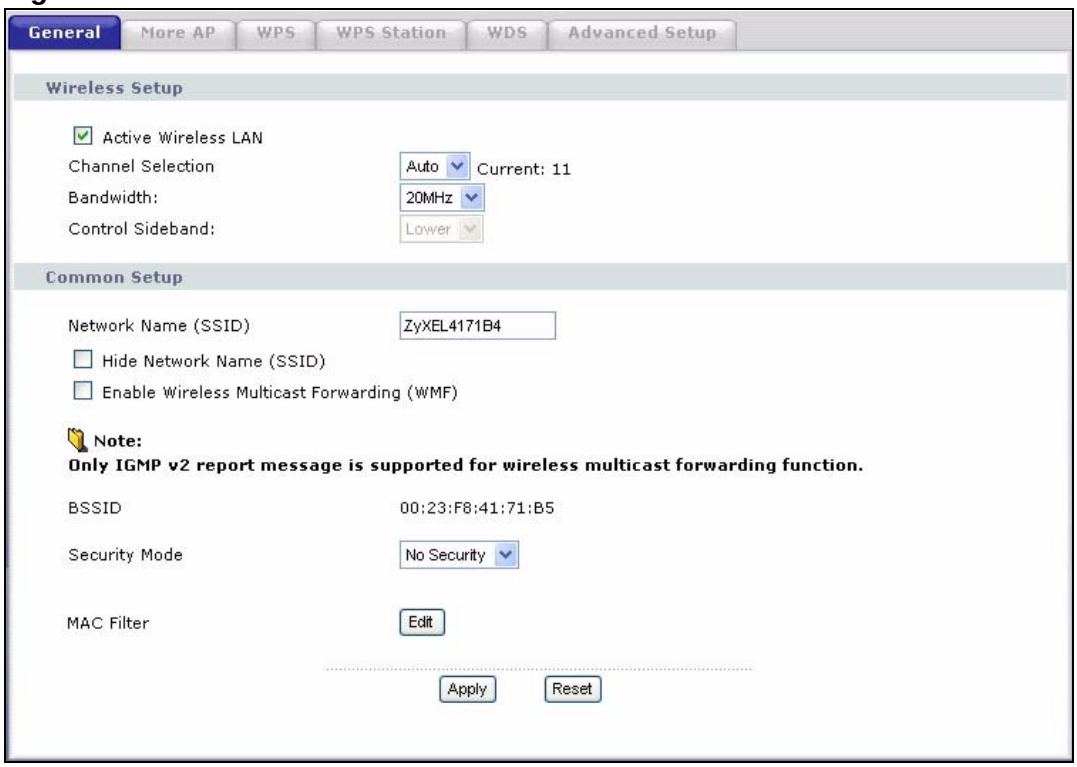
  Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.
- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

7.4 The General Screen

Note: If you are configuring the P-2812HNU-51c from a computer connected to the wireless LAN and you change the P-2812HNU-51c's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the P-2812HNU-51c's new settings.

Click **Network > Wireless LAN** to open the **General** screen.

Figure 60 Network > Wireless LAN > General



The following table describes the labels in this screen.

Table 34 Network > Wireless LAN > General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate wireless LAN.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel or use **Auto** to have the P-2812HNU-51c automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the P-2812HNU-51c is currently using then displays next to this field.

Table 34 Network > Wireless LAN > General

LABEL	DESCRIPTION
Bandwidth	Select whether the P-2812HNU-51c uses a wireless channel width of **20MHz** or **40MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. This field is available only when you set the **802.11 Mode** to **802.11n Only** or **802.11b/g/n Mixed** in the **Advanced Setup** screen.
Control Sideband	This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands. This field is available only when you set the **802.11 Mode** to **802.11n Only** or **802.11b/g/n Mixed** in the **Advanced Setup** screen.
Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the P-2812HNU-51c from a computer connected to the wireless LAN and you change the P-2812HNU-51c's SSID or wireless security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the P-2812HNU-51c's new settings.
Hide Network Name (SSID)	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Enable Wireless Multicast Forwarding (WMF)	Select this check box to allow the P-2812HNU-51c to convert wireless multicast traffic into wireless unicast traffic.
BSSID	This shows the MAC address of the wireless interface on the P-2812HNU-51c when wireless LAN is enabled.
Security Mode	See the following sections for more details about this field.
MAC Filter	Click this button to go to the **MAC Filter** screen to configure whether the wireless devices with the MAC addresses listed are allowed or denied to access the P-2812HNU-51c using this SSID.

Table 34 Network > Wireless LAN > General

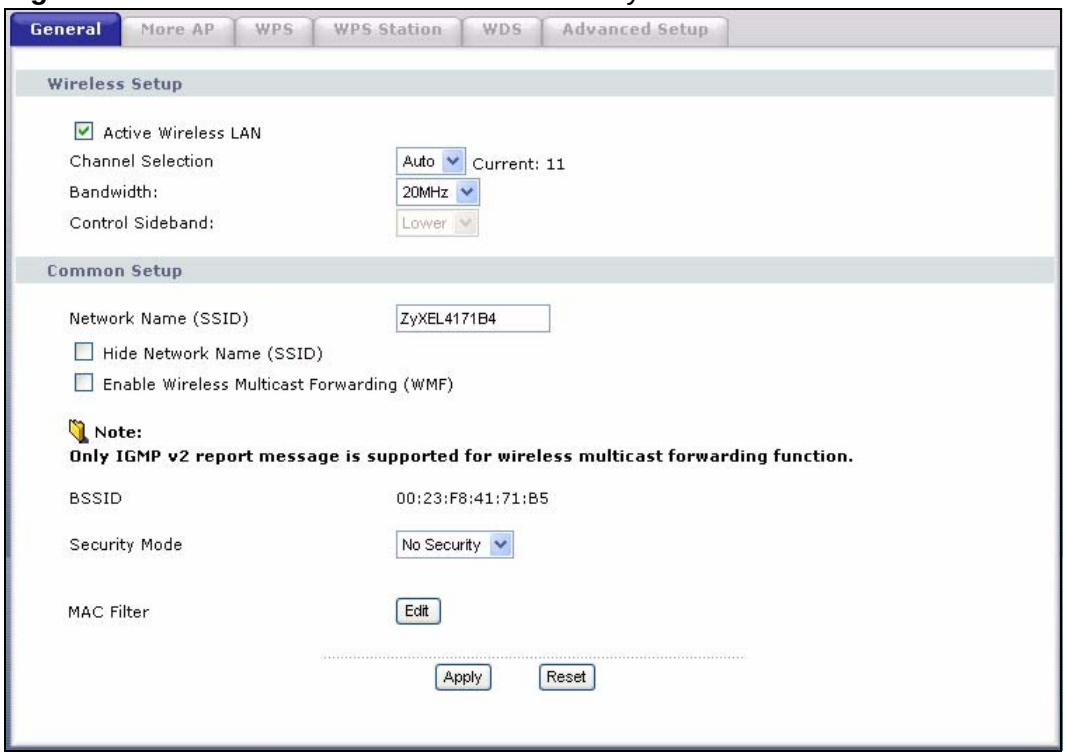
LABEL	DESCRIPTION
Apply	Click this to save your changes back to the P-2812HNU-51c.
Reset	Click this to reload the previous configuration for this screen.

7.4.1 No Security

Select **No Security** to allow wireless devices to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your P-2812HNU-51c, your network is accessible to any wireless networking device that is within range.

Figure 61 Wireless LAN > General: No Security



The following table describes the labels in this screen.

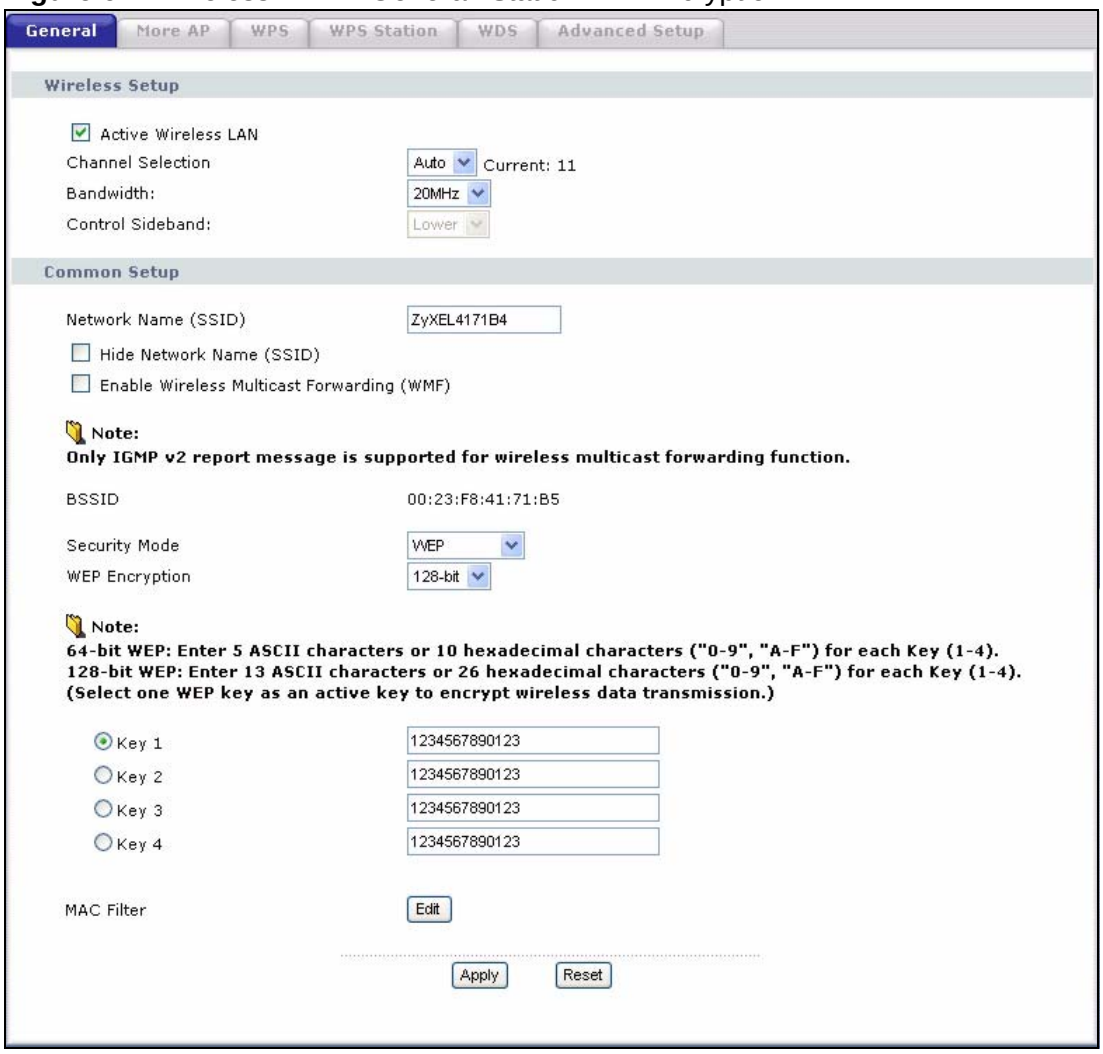
Table 35 Wireless LAN > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.

7.4.2 WEP Encryption

In order to configure and enable WEP encryption; click **Network > Wireless LAN** to display the **General** screen. Select **WEP** from the **Security Mode** list.

Figure 62 Wireless LAN > General: Static WEP Encryption



The following table describes the wireless LAN security labels in this screen.

Table 36 Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose **WEP** from the drop-down list box.

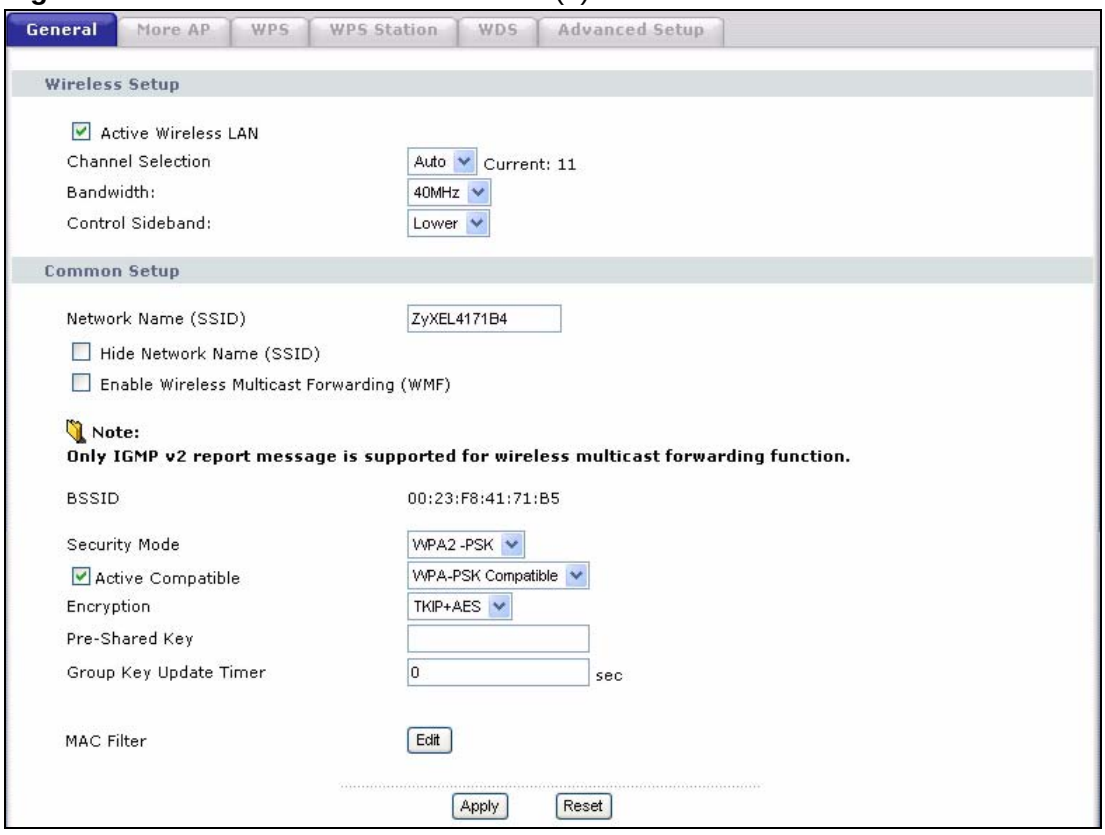
Table 36 Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **64-bit** or **128-bit** to enable data encryption.
Key 1 to Key 4	The WEP key is used to secure your data from eavesdropping by unauthorized wireless users. Both the P-2812HNU-51c and the wireless stations must use the same WEP key for data transmission. Only one key can be activated at any one time. Select a default key to use for data encryption. If you chose **64-bit** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.

7.4.3 WPA(2)-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 63 Wireless LAN > General: WPA(2)-PSK



The following table describes the wireless LAN security labels in this screen.

Table 37 Wireless LAN > General: WPA(2)-PSK

LABEL	DESCRIPTION
Auto Generate Key	This field is only available for WPA-PSK. Select this option to have the P-2812HNU-51c automatically generate an SSID and pre-shared key. The **SSID** and **Pre-Shared Key** fields will not be configurable when you select this option.
Security Mode	Choose **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Active Compatible	This field is only available for WPA2-PSK. Select this if you want the P-2812HNU-51c to support WPA-PSK and WPA2-PSK simultaneously.
Encryption	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **TKIP** if your wireless clients can all use TKIP. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.
Pre-Shared Key	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients.

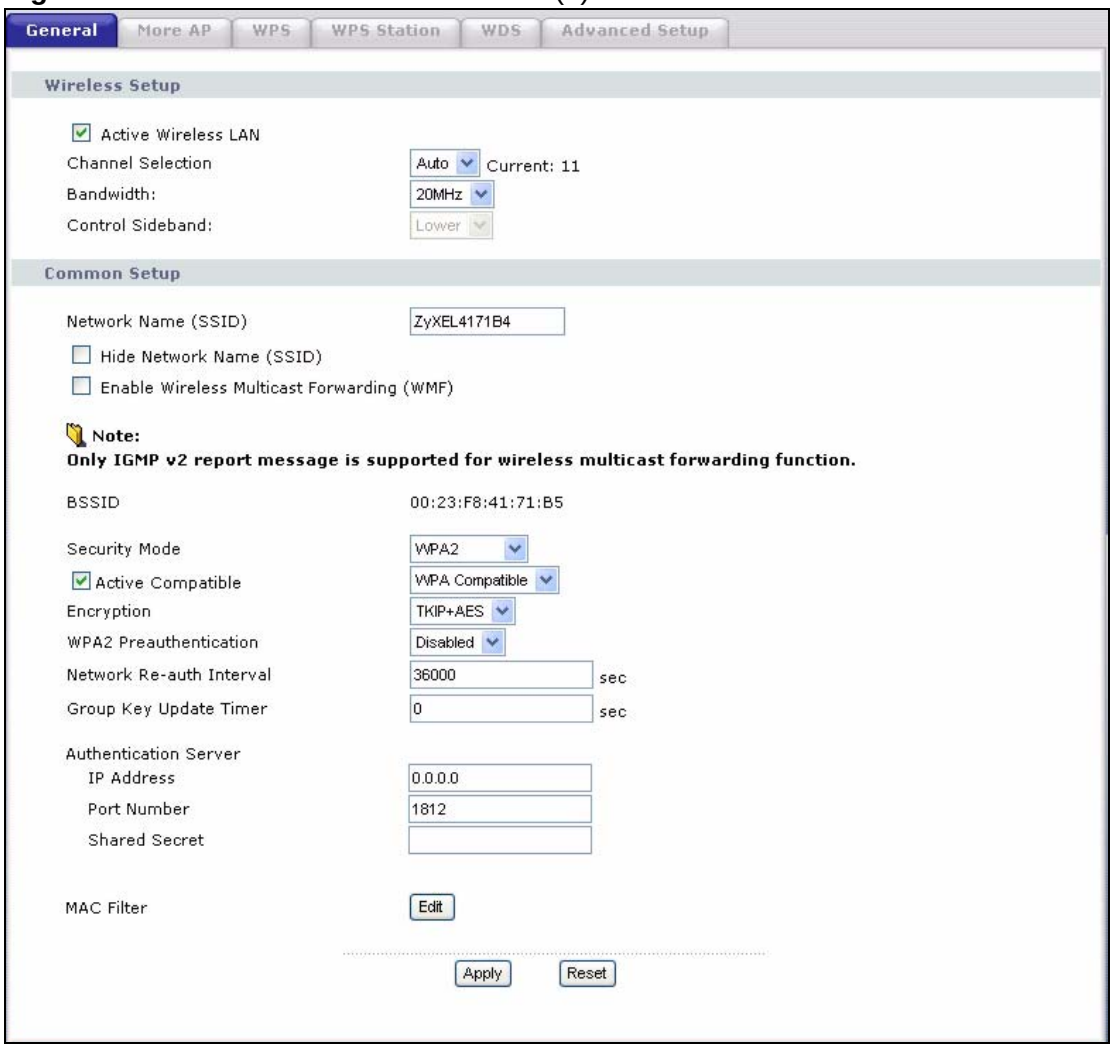
7.4.4 WPA(2) Authentication

Use this screen to configure and enable WPA or WPA2 authentication; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Note: WPA or WPA2 is not available if you enable WPS before you configure WPA or WPA2 in the **Wireless LAN** > **General** screen.

Note: If you select **WPA** or **WPA2** in the **Wireless LAN > General** screen, the WDS and WPS features are not available on the P-2812HNU-51c.

Figure 64 Wireless LAN > General: WPA(2)



The following table describes the wireless LAN security labels in this screen.

Table 38 Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
Active Compatible	This field is only available for WPA2. Select this if you want the P-2812HNU-51c to support WPA and WPA2 simultaneously.
Encryption	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **TKIP** if your wireless clients can all use TKIP. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.

Table 38 Wireless LAN > General: WPA(2)

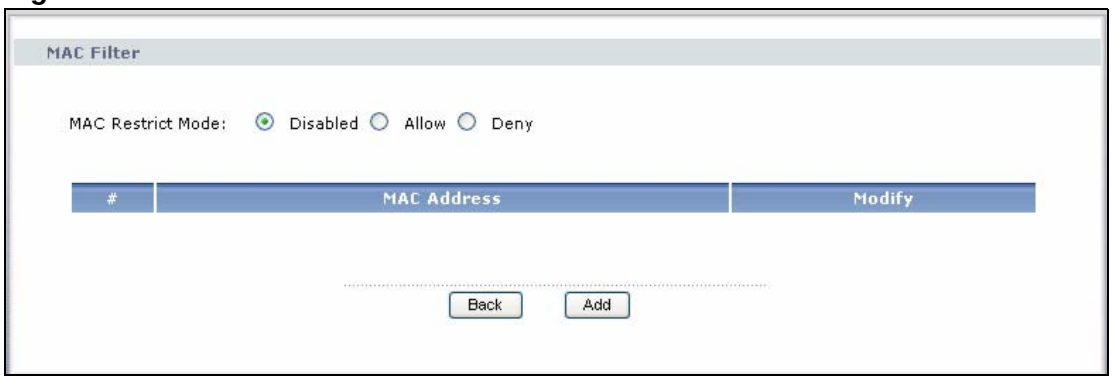
LABEL	DESCRIPTION
WPA2 Preauthentication	This field is available only when you select **WPA2**. Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select **Enabled** to turn on preauthentication in WAP2. Otherwise, select **Disabled**.
Network Re-auth Interval	This field is available only when you select **WPA2**. Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 2147483647 seconds. Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the P-2812HNU-51c. The key must be the same on the external authentication server and your P-2812HNU-51c. The key is not sent over the network.

7.4.5 MAC Filter

This screen allows you to configure the P-2812HNU-51c to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the P-2812HNU-51c (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use this screen to change your P-2812HNU-51c's MAC filter settings. Click the **Edit** button in the **Wireless LAN > General** screen. The following screen displays.

Figure 65 Wireless LAN > MAC Filter



The following table describes the labels in this screen.

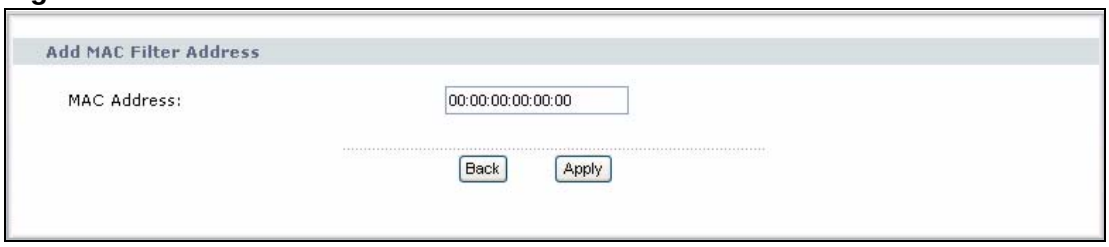
Table 39 Wireless LAN > MAC Filter

LABEL	DESCRIPTION
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the table below. Select **Disabled** to turn off MAC address filtering. Select **Allow** to permit access to the P-2812HNU-51c, MAC addresses not listed will be denied access to the P-2812HNU-51c. Select **Deny** to block access to the P-2812HNU-51c, MAC addresses not listed will be allowed to access the P-2812HNU-51c
#	This is the index number of the MAC address.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the P-2812HNU-51c.
Modify	Click the **Remove** icon to delete the entry.
Back	Click this to return to the previous screen without saving changes.
Add	Click this to create a new MAC filtering rule.

7.4.6 Adding a New MAC Filtering Rule

Click the **Add** button in the **MAC Filter** screen. The following screen displays.

Figure 66 Wireless LAN > MAC Filter > Add



The following table describes the labels in this screen.

Table 40 Wireless LAN > MAC Filter > Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the P-2812HNU-51c in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Back	Click this to return to the previous screen without saving changes.
Apply	Click this to save your changes and go back to the previous screen.

7.5 The More AP Screen

This screen allows you to enable and configure multiple wireless networks on the P-2812HNU-51c.

Click **Network > Wireless LAN** > **More AP**. The following screen displays.

Figure 67 Network > Wireless LAN > More AP

The following table describes the labels in this screen.

Table 41 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Active	Select the check box to activate an SSID profile.
SSID	An SSID profile is the set of parameters relating to one of the P-2812HNU-51c's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the **Edit** icon to configure the SSID profile.

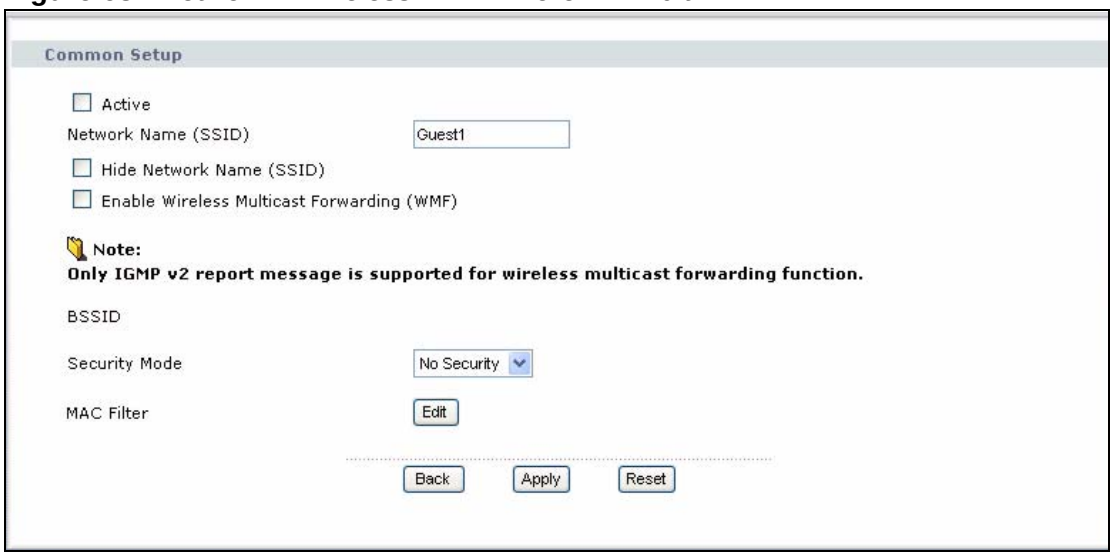
Table 41 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.1 More AP Edit

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 68 Network > Wireless LAN > More AP: Edit



See Section 7.4 on page 153 for more details about the fields in this screen.

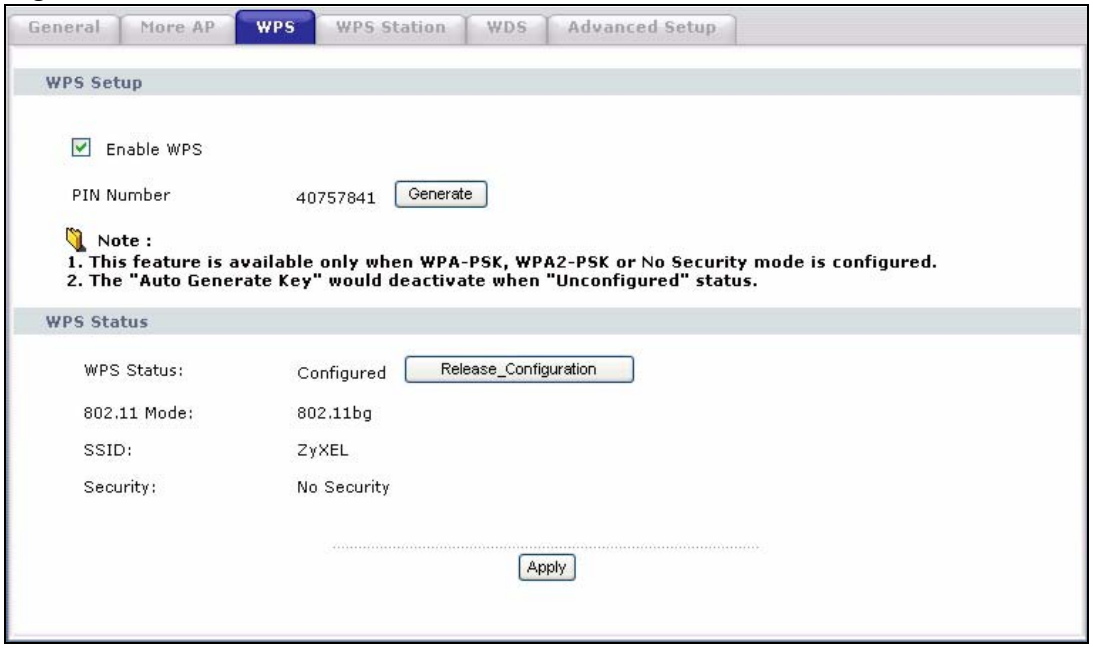
7.6 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your P-2812HNU-51c.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS.

Click **Network > Wireless LAN >WPS**. The following screen displays.

Figure 69 Network > Wireless LAN > WPS



The following table describes the labels in this screen.

Table 42 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select the check box to activate WPS on the P-2812HNU-51c.
PIN Number	This shows the PIN (Personal Identification Number) of the P-2812HNU-51c. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method.
Generate	Click this button to have the P-2812HNU-51c create a new PIN.
WPS Status	This displays **Configured** when the P-2812HNU-51c has connected to a wireless network using WPS or **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there is no wireless or wireless security changes on the P-2812HNU-51c or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release_Configuration	This button is available when the WPS status is **Configured** but not configurable if you disable WPS. Click this button to remove all configured wireless and wireless security settings for WPS connections on the P-2812HNU-51c.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.

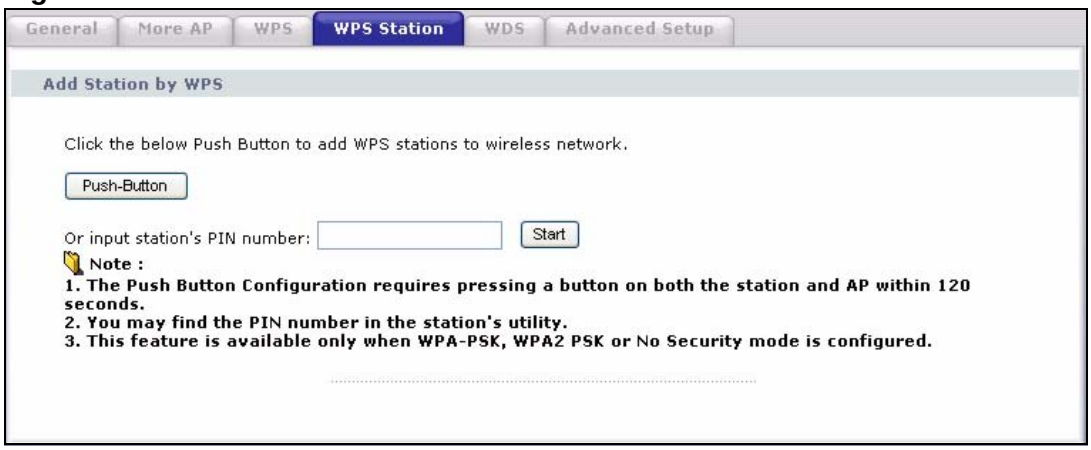
7.7 The WPS Station Screen

Use this screen to set up a WPS wireless network using either Push Button Configuration (PBC) or PIN Configuration.

Note: If you select **No Security** in the **Wireless LAN > General** screen and click **Push Button** in the **WPS Station** screen, the P-2812HNU-51c automatically changes to use WPA-PSK/WPA2-PSK mixed mode and generates a pre-shared key.

Click **Network > Wireless LAN > WPS Station**. The following screen displays.

Figure 70 Network > Wireless LAN > WPS Station


General
More AP
WPS
WPS Station
WDS
Advanced Setup
Add Station by WPS
Click the below Push Button to add WPS stations to wireless network.
Push-Button
Or input station's PIN number:
Start
Note :
1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.
3. This feature is available only when WPA-PSK, WPA2 PSK or No Security mode is configured.

The following table describes the labels in this screen.

Table 43 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Click this button to add another WPS-enabled wireless device (within wireless range of the P-2812HNU-51c) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **Push Button** on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Or input station's PIN number	Enter the PIN of the device that you are setting up a WPS connection with and click **Start** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the P-2812HNU-51c.

7.8 The WDS Screen

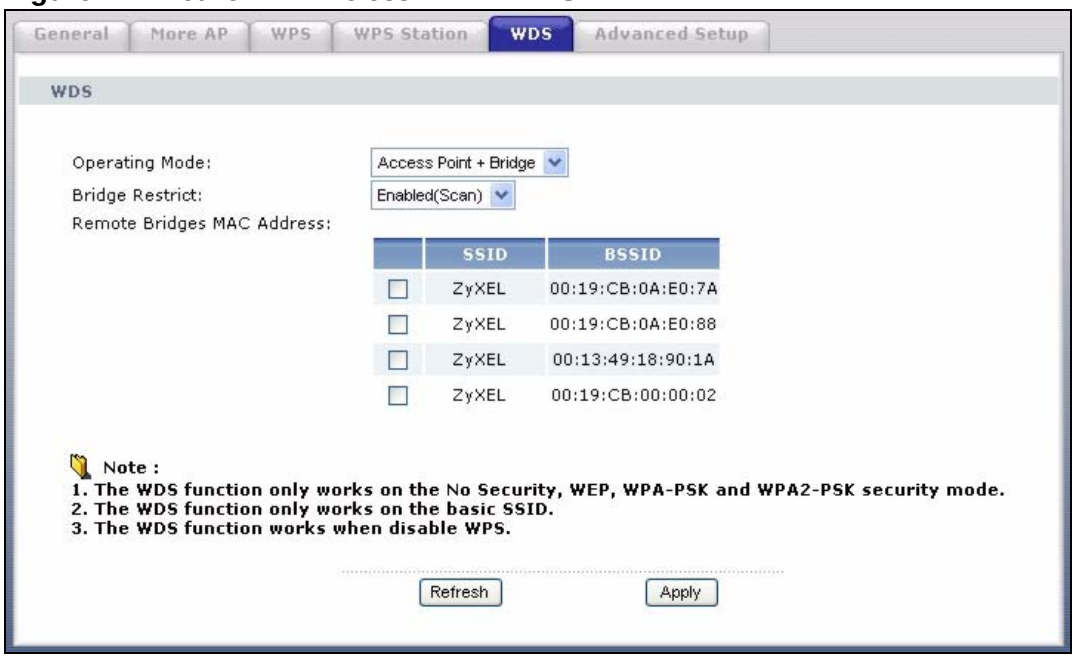
A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Use this screen to set up your WDS links between the P-2812HNU-51cs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between the devices is made.

Note: You cannot use WDS when WPS is enabled or wireless security is set to “WPA" or "WPA2". The wireless security settings apply to both WDS links and the connections between the ZyXEL Device and any wireless clients.

Note: At the time of writing, WDS is only compatible with other ZyXEL Devices of the same model.

Click **Network > Wireless LAN > WDS**. The following screen displays. WDS is turned on and this screen is configurable when the ZyXEL Device's wireless security mode is **No Security**, **WEP** or **WPA**(**2**)**-PSK**.

Figure 71 Network > Wireless LAN > WDS



The following table describes the labels in this screen.

Table 44 Network > Wireless LAN > WDS

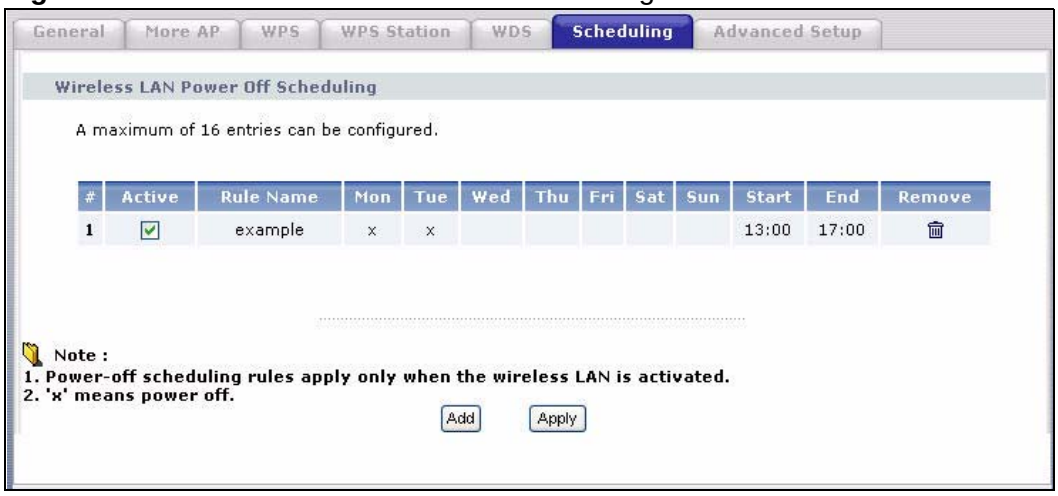
LABEL	DESCRIPTION
WDS	
Operating Mode	Select the operating mode for your P-2812HNU-51c. • **Access Point + Bridge -** The P-2812HNU-51c functions as a bridge and access point simultaneously. • **Wireless Bridge** - The P-2812HNU-51c acts as a wireless network bridge and establishes wireless links with other APs. In this mode, clients cannot connect to the P-2812HNU-51c wirelessly. You need to know the MAC address of the peer device, which must be of the same model and also WDS-enabled. The P-2812HNU-51c can establish up to four wireless links with other APs.
Bridge Restrict	This field is available only when you set operating mode to **Access Point + Bridge**. Select **Enabled** to turn on WDS and enter the peer device's MAC address manually in the table below. Select **Enabled(Scan)** to turn on WDS, search and display the available APs within range in the table below.
Remote Bridges MAC Address	Enter the MAC address of the peer device that your P-2812HNU-51c wants to make a bridge connection with. You can connect to up to 4 peer devices.
	This field is available only when you select **Enabled(Scan)** in the **Bridge Restrict** field. Select the check box and click **Apply** to have the P-2812HNU-51c establish a wireless link with the selected wireless device.
SSID	This field is available only when you select **Enabled(Scan)** in the **Bridge Restrict** field. This shows the SSID of the available wireless device within range.
BSSID	This field is available only when you select **Enabled(Scan)** in the **Bridge Restrict** field. This shows the MAC address of the available wireless device within range.
Refresh	Click **Refresh** to update the **Remote Bridges MAC Address** table when **Bridge Restrict** is set to **Enabled(Scan)**.
Apply	Click **Apply** to save your changes to the P-2812HNU-51c.

7.9 The Wireless Scheduling Screen

The wireless LAN can be scheduled to disable on certain days and at certain times. Use this screen to view the wireless scheduling rules and enable or disable a rule on the P-2812HNU-51c. To open this screen, click **Network** > **Wireless LAN** > **Scheduling**.

Note: Using the **Wireless LAN > General** screen or the WPS button to turn off or on the wireless LAN has priority over wireless power-off scheduling.

Figure 72 Network > Wireless LAN > Scheduling


General
More AP
WPS
WPS Station
WDS
Scheduling
Advanced Setup
Wireless LAN Power Off Scheduling
A maximum of 16 entries can be configured.
Active Rule Name Mon Tue Wed Thu Fri Sat Sun Start End Remove
1 example x x 13:00 17:00
Note :
1. Power-off scheduling rules apply only when the wireless LAN is activated.
2. 'x' means power off.
Add
Apply

The following table describes the labels in this screen.

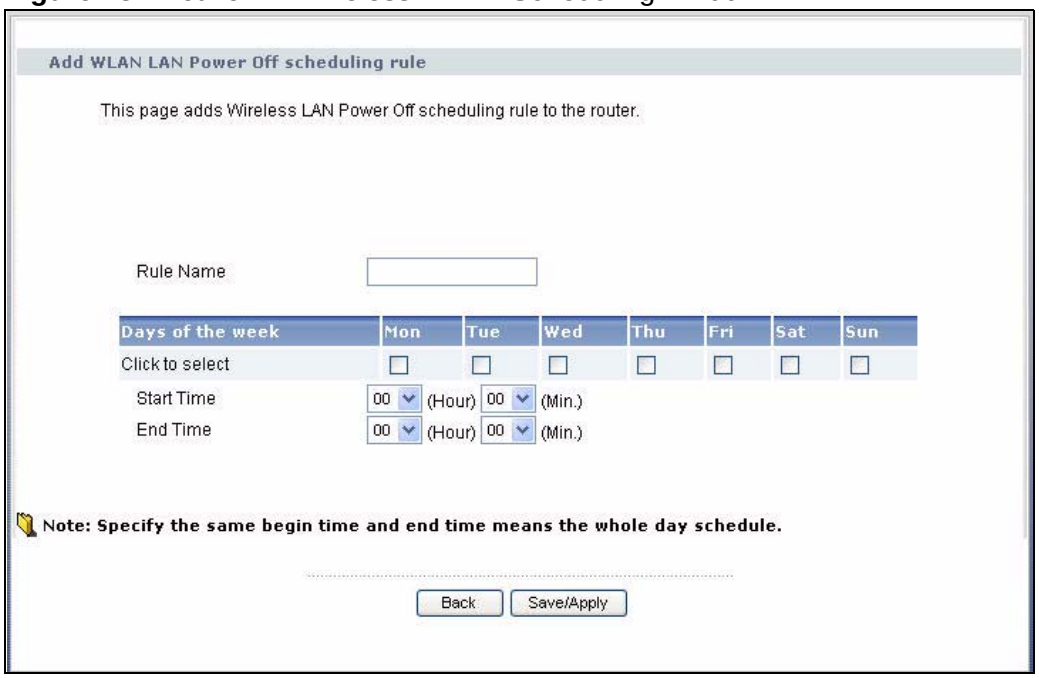
Table 45 Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Wireless LAN Power Off Scheduling	
#	This field displays the index number of a rule.
Active	Select the check box to enable a rule. Otherwise, clear the check box to disable a rule without deleting it.
Rule Name	This field displays the descriptive name of a rule.
Mon Tue Wed Thu Fri Sat Sun	This field displays whether wireless power-off scheduling is active on the day(s). **x** means the P-2812HNU-51c turns off the wireless LAN in the specified time period of the day(s).
Start	This field displays the time of day when power-off scheduling starts and the P-2812HNU-51c turns off the wireless LAN.
End	This field displays the time of day when power-off scheduling ends and the P-2812HNU-51c turns on the wireless LAN again.
Remove	Click the icon to delete a rule.
Add	Click **Add** to create a new scheduling rule.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.

7.9.1 Adding a WLAN Power-off Scheduling Rule

Use this screen to set the times your wireless LAN is turned off. To open this screen, click the **Add** button in the **Wireless LAN** > **Scheduling** screen.

Figure 73 Network > Wireless LAN > Scheduling > Add



The following table describes the labels in this screen.

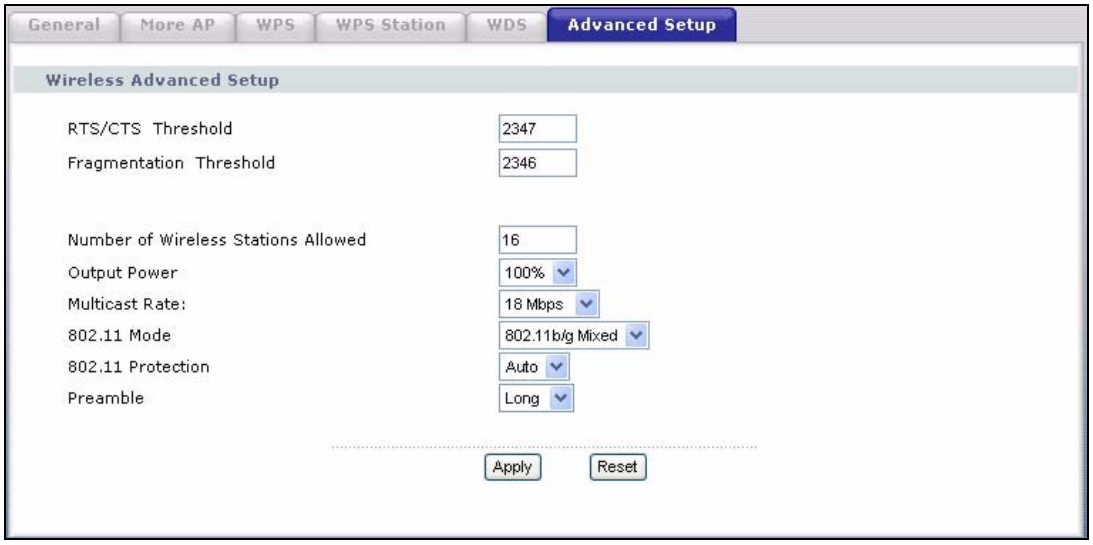
Table 46 Network > Wireless LAN > Scheduling > Add

LABEL	DESCRIPTION
Rule Name	Enter a descriptive name for identification purposes. You can enter up to 15 alphanumeric characters. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Days of the week	Select which day(s) of the week you want wireless power-off scheduling to be active.
Start Time	Select a begin time using the **Hour** and minute (**Min.**) drop down boxes. The wireless LAN will turn off between the start time and end time you specified.
End Time	Select an end time using the **Hour** and minute (**Min.**) drop down boxes.
Back	Click **Back** to return to the previous screen.
Save/Apply	Click **Save/Apply** to save your changes back to the P-2812HNU-51c.

7.10 The Advanced Setup Screen

To configure advanced wireless settings, click **Network > Wireless LAN > Advanced Setup**. The screen appears as shown.

Figure 74 Wireless LAN > Advanced Setup



The following table describes the labels in this screen.

Table 47 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
RTS/CTS Threshold	Enter a value between 0 and 2432.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Number of Wireless Stations Allowed	Specify the maximum number (from 1 to 64) of the wireless stations that may connect to the P-2812HNU-51c.
Output Power	Set the output power of the P-2812HNU-51c. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following **20%**, **40%**, **60%**, **80%** or **100%**.
Multicast Rate	Select a data rate at which the P-2812HNU-51c transmits wireless multicast traffic. If you select a high rate, multicast traffic may occupy all the bandwidth and cause network congestion.

Table 47 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
802.11 Mode	Select **802.11b Only** to only allow IEEE 802.11b compliant WLAN devices to associate with the P-2812HNU-51c. Select **802.11g Only** to allow IEEE 802.11g compliant WLAN devices to associate with the P-2812HNU-51c. IEEE 802.11b compliant WLAN devices can associate with the P-2812HNU-51c only when they use the short preamble type. Select **802.11n Only** to only allow IEEE 802.11n compliant WLAN devices to associate with the P-2812HNU-51c. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the P-2812HNU-51c. Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the P-2812HNU-51c. The P-2812HNU-51c adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. Select **802.11 b/g/n Mixed** to allow both IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the P-2812HNU-51c. The transmission rate of your P-2812HNU-51c might be reduced.
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your P-2812HNU-51c might be reduced in a mixed-mode network. This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long** or **Short**. The default setting is **Long**. See the appendix for more information. This field is not configurable and the P-2812HNU-51c uses **Short** when you set **802.11 Mode** to **802.11g Only**, **802.11n Only** or **802.11b/g/n Mixed**.
Apply	Click this to save your changes back to the P-2812HNU-51c.
Reset	Click this to reload the previous configuration for this screen.

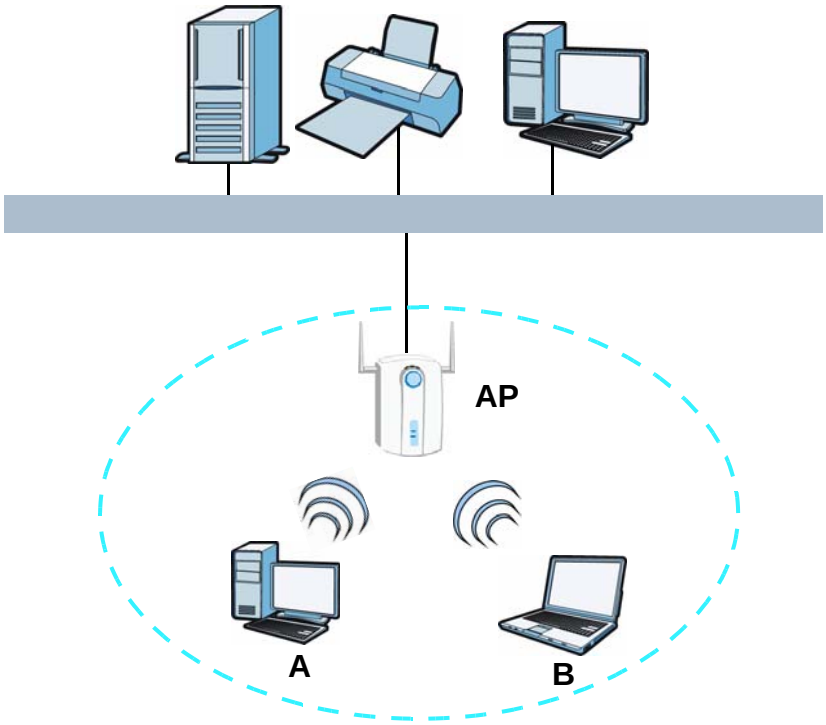
7.11 Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

7.11.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 75 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your P-2812HNU-51c is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

7.11.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the P-2812HNU-51c's Web Configurator.

Table 48 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the P-2812HNU-51c. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the P-2812HNU-51c.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the P-2812HNU-51c does, it cannot communicate with the P-2812HNU-51c.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

7.11.3 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

7.11.3.1 SSID

Normally, the P-2812HNU-51c acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the P-2812HNU-51c does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

7.11.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal

characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the P-2812HNU-51c which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

7.11.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

7.11.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

The types of encryption you can choose depend on the type of authentication. (See Section 7.11.3.3 on page 174 for information about this.)

Table 49 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	
↕	Static WEP	
	WPA-PSK	WPA
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the P-2812HNU-51c and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your P-2812HNU-51c, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the P-2812HNU-51c.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

7.11.4 WiFi Protected Setup

Your P-2812HNU-51c supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works

between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

7.11.4.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the P-2812HNU-51c, see Section 7.7 on page 165).
3. Press the button on one of the devices (it doesn't matter which). For the P-2812HNU-51c you must press the WPS button for more than three seconds.
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

7.11.4.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
3. Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the P-2812HNU-51c, see Section 7.6 on page 163).
4. Enter the client's PIN in the AP's configuration interface.

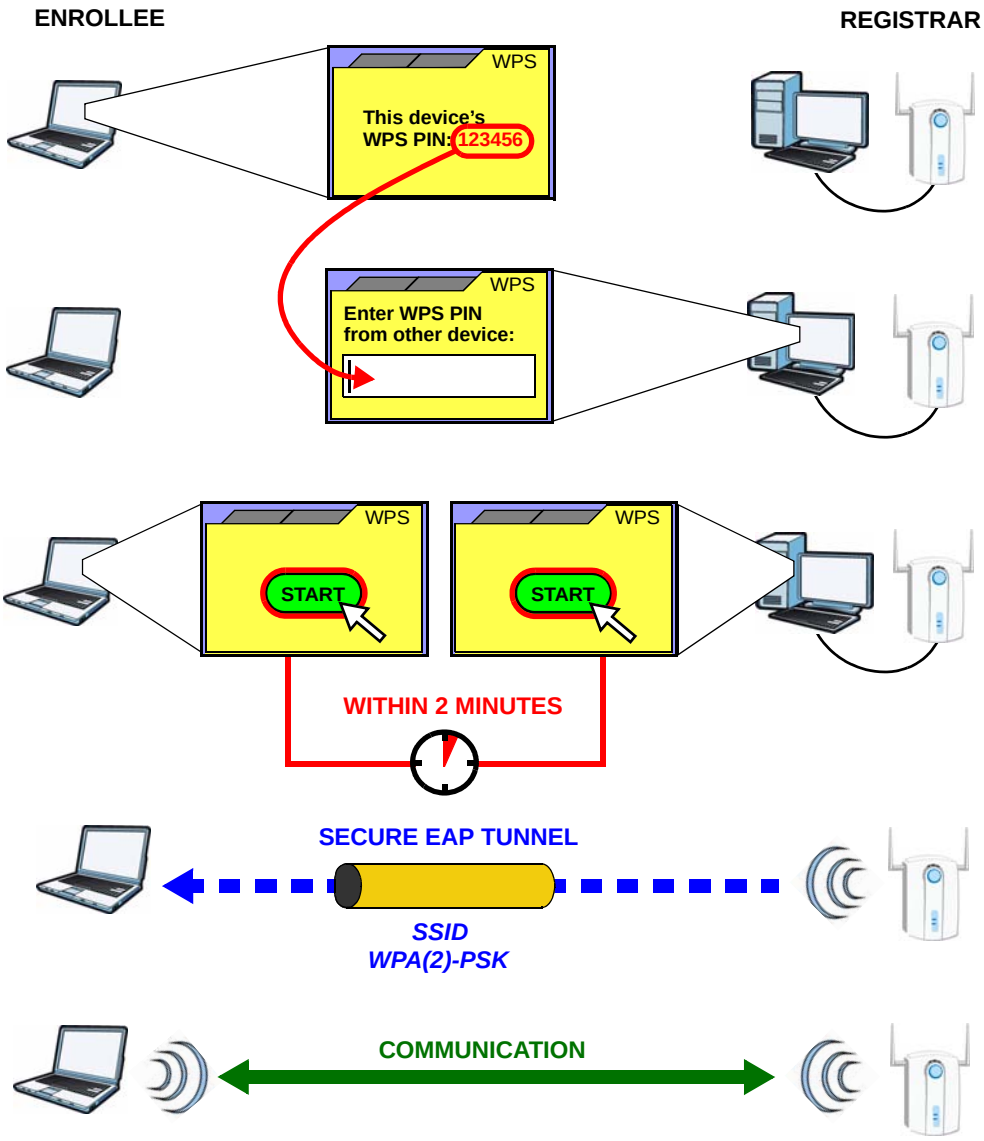
   Note: If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
5. Start WPS on both devices within two minutes.

   Note: Use the configuration utility to activate WPS, not the push-button on the device itself.
6. On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

   If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 76 Example WPS Process: PIN Method

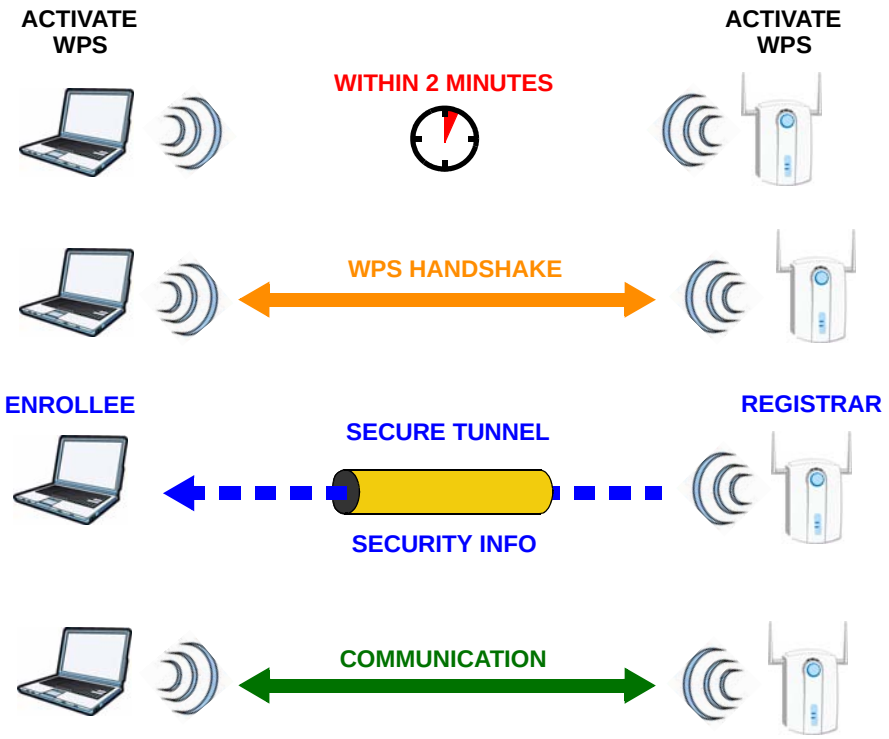


7.11.4.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 77 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

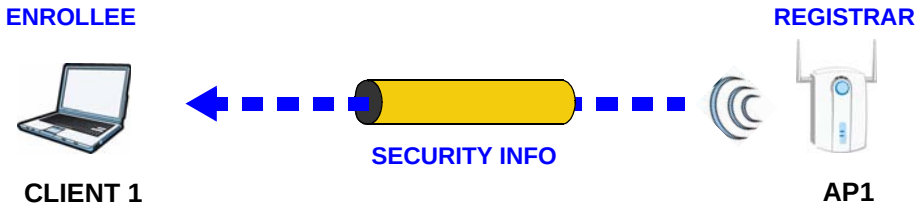
By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

7.11.4.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

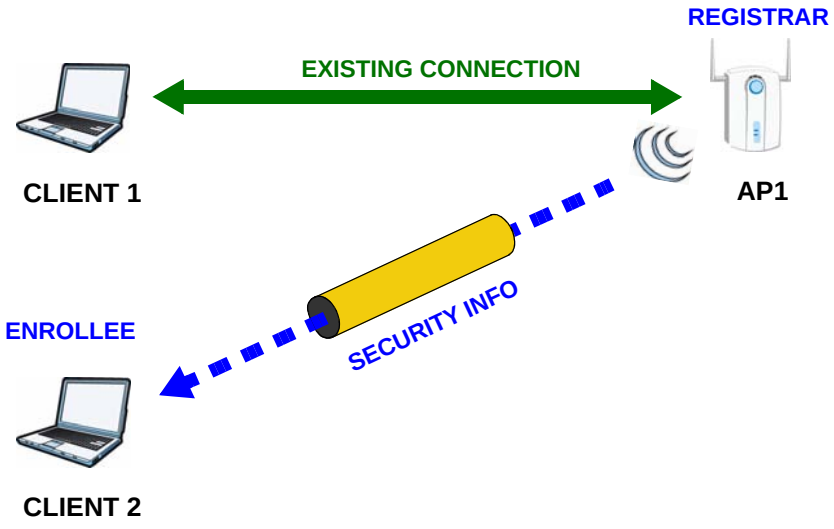
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 78 WPS: Example Network Step 1



In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

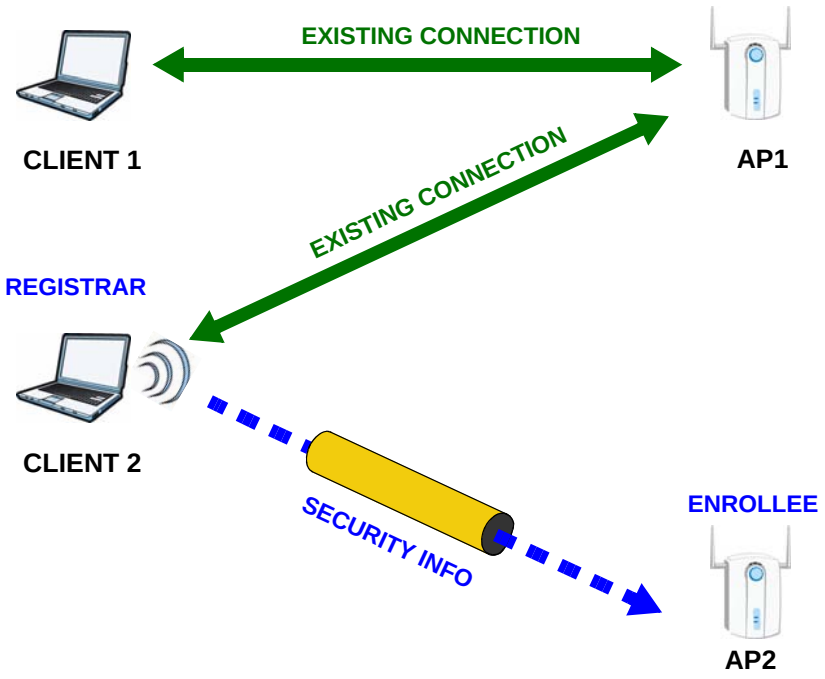
Figure 79 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access

point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 80 WPS: Example Network Step 3



7.11.4.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

8

Network Address Translation (NAT)

8.1 Overview

This chapter discusses how to configure NAT on the P-2812HNU-51c.

Network Address Translation (NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.1.1 What You Can Do in this Chapter

- The **Port Forwarding** screen lets you configure forward incoming service requests to the server(s) on your local network (Section 8.3 on page 184).
- The **Trigger Port** screen lets you change the P-2812HNU-51c's trigger port settings (Section 8.4 on page 187).
- The **DMZ Host** screen lets you configure a default server (Section 8.5 on page 192).
- The **ALG** screen lets you enable SIP ALG on the P-2812HNU-51c (Section 8.6 on page 192).

8.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

8.3 The Port Forwarding Screen

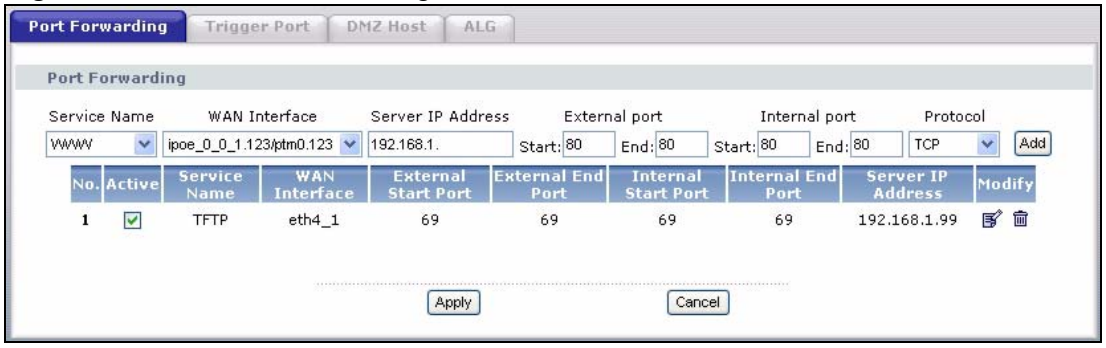
This summary screen provides a summary of all port forwarding rules and their configuration. In addition, this screen allows you to create new port forwarding rules and delete existing rules.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

To access this screen, click **Network > NAT**. The following screen appears.

Figure 81 NAT Port Forwarding



The following table describes the labels in this screen.

Table 50 NAT Port Forwarding

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will display in the **External port**, **Internal port** and **Protocol** fields. Otherwise, select **User Define** to open the **Rule Setup** screen where you can manually enter the port number(s) and select the IP protocol.
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
Server IP Address	Enter the IP address of the server for the specified service.
External Port Start	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External Port End** field. To forward a series of ports, enter the start port number here and the end port number in the **External Port End** field.
External Port End	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Port Start** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Port Start** field above.
Internal Port Start	Enter the port number to which you want the P-2812HNU-51c to translate the incoming port. To forward only one port, enter the port number again in the **Internal Port End** field. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Internal Port End	Enter the last port of the translated port range.
Protocol	This is the transport layer protocol used for the service.
Add	Click this button to add a rule to the table below.
No.	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Server Name	This field displays the name of the service used by the packets for this virtual server.
WAN Interface	This field displays the WAN interface through which the service is forwarded.
External Start Port	This is the first external port number that identifies a service.
External End Port	This is the last external port number that identifies a service.

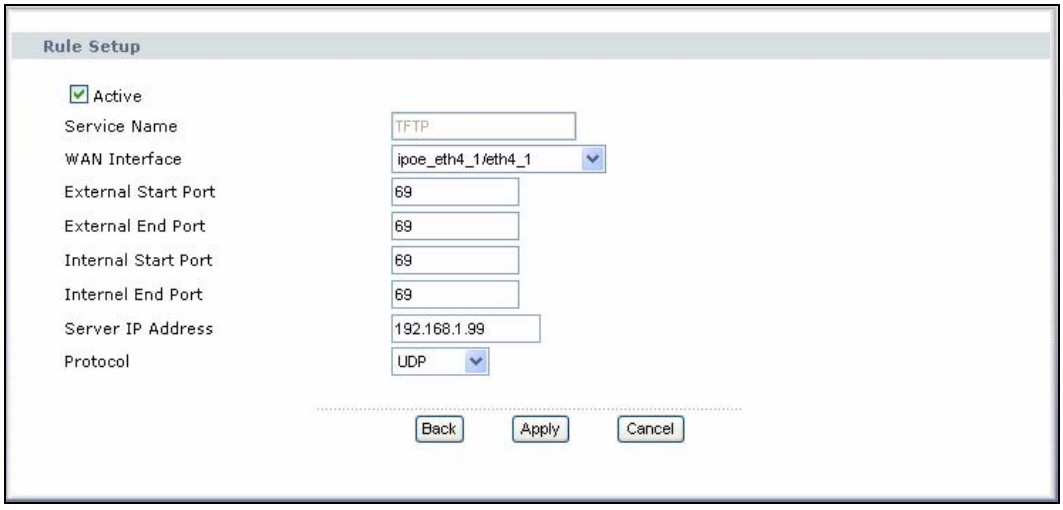
Table 50 NAT Port Forwarding (continued)

LABEL	DESCRIPTION
Internal Start Port	This is the first internal port number that identifies a service.
Internal End Port	This is the last internal port number that identifies a service.
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the **Edit** icon to go to the screen where you can edit the port forwarding rule. Click the **Remove** icon to delete an existing port forwarding rule. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to return to the previous configuration.

8.3.1 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Select **User Define** in the **Service Name** field or click the rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.

Figure 82 Port Forwarding Edit



The following table describes the labels in this screen.

Table 51 Port Forwarding Edit

LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it. This field is not editable if you are configuring a **User Define** rule.
Service Name	Enter a name to identify this rule. This field is read-only if you click the **Edit** icon in the **Port Forwarding** screen.

Table 51 Port Forwarding Edit (continued)

LABEL	DESCRIPTION
WAN Interface	Select a WAN interface for which you want to configure port forwarding rules.
External Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.
External End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above.
Internal Start Port	Enter the port number here to which you want the P-2812HNU-51c to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Internal End Port	Enter the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the transport layer protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.4 The Trigger Port Screen

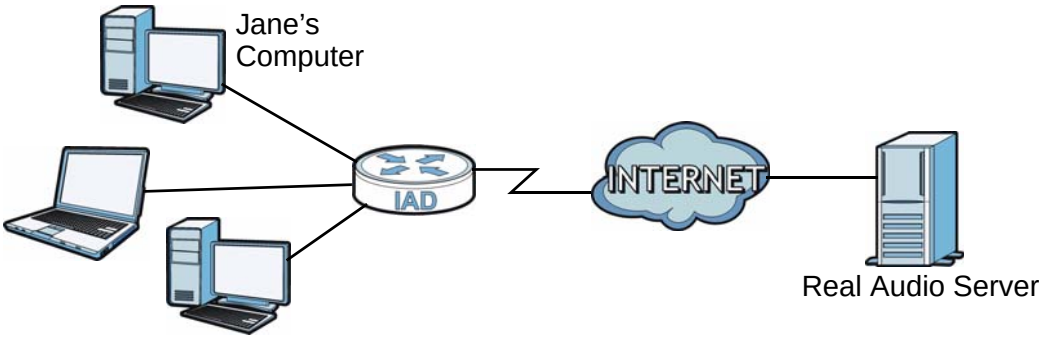
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The P-2812HNU-51c records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the P-2812HNU-51c's WAN port receives a response with a specific port number and protocol ("open"

port), the P-2812HNU-51c forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

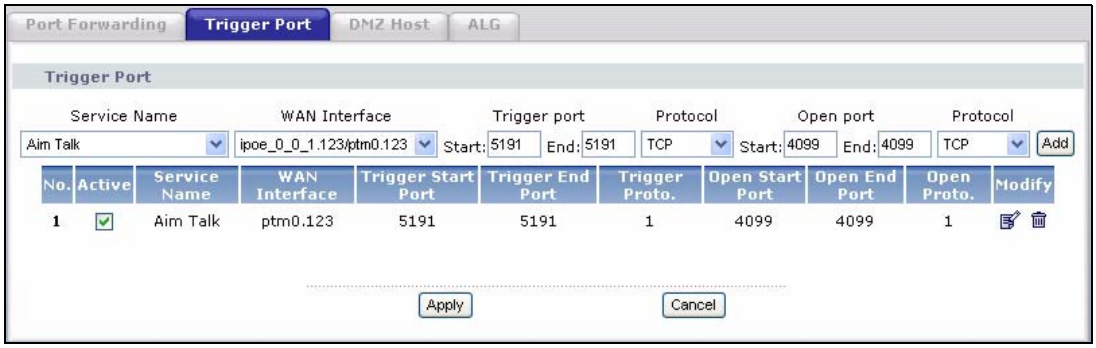
Figure 83 Trigger Port Forwarding Process: Example



1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the P-2812HNU-51c to record Jane's computer IP address. The P-2812HNU-51c associates Jane's computer IP address with the "open" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The P-2812HNU-51c forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The P-2812HNU-51c times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **NAT** > **Trigger Port** to open the following screen. Use this screen to view and configure your P-2812HNU-51c's trigger port settings.

Figure 84 Trigger Port



The following table describes the labels in this screen.

Table 52 NAT Trigger Port

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will display in the **Trigger port**, **Open port** and **Protocol** fields. Otherwise, select **User Define** to open the **Rule Setup** screen where you can manually enter the port number(s) and select the transport layer protocol.
WAN Interface	Select the WAN interface through which the service is forwarded.
Trigger Port	The trigger port is a port (or a range of ports) that causes (or triggers) the P-2812HNU-51c to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start	This is the first port number that identifies a service.
End	This is the last port number that identifies a service.
Protocol	This is the transport layer protocol used for the service.
Open Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The P-2812HNU-51c forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start	This is the first port number that identifies a service.
End	This is the last port number that identifies a service.
Protocol	This is the transport layer protocol used for the service.
Add	Click this button to add a rule to the table below.
No.	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Server Name	This field displays the name of the service used by the packets for this virtual server.
WAN Interface	This field displays the WAN interface through which the service is forwarded.

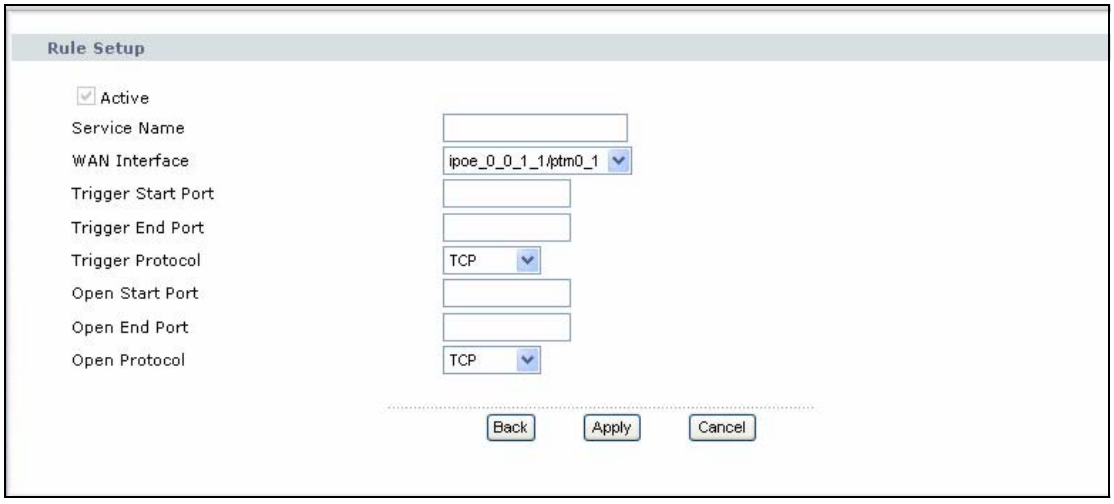
Table 52 NAT Trigger Port (continued)

LABEL	DESCRIPTION
Trigger Start Port	This is the first trigger port number that identifies a service.
Trigger End Port	This is the last trigger port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol. **1** means TCP, **2** means UDP and **3** means TCP/UDP.
Open Start Port	This is the first open port number that identifies a service.
Open End Port	This is the last open port number that identifies a service.
Open Proto.	This is the open transport layer protocol. **1** means TCP, **2** means UDP and **3** means TCP/UDP.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Remove** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to return to the previous configuration.

8.4.1 Trigger Port Configuration

This screen lets you create new port triggering rules. Click the **Add** icon in the **NAT - Trigger Port** screen to open the following screen.

Figure 85 NAT > Trigger Port > Add



The following table describes the labels in this screen.

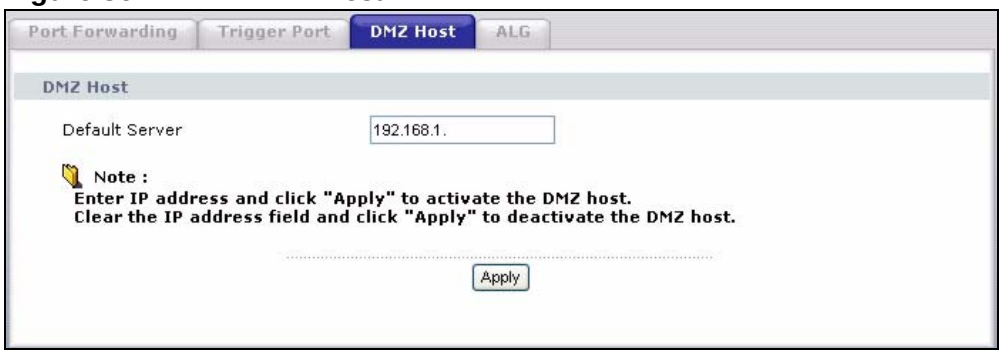
Table 53 NAT > Port Triggering > Add

LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it. This field is not editable if you are configuring a **User Define** rule.
Service Name	Enter a name to identify this rule. This field is read-only if you click the **Edit** icon in the **Trigger Port** screen.
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the P-2812HNU-51c to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The P-2812HNU-51c forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.5 The DMZ Host Screen

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in the **NAT Port Forwarding Setup** screen.

Figure 86 NAT > DMZ Host



The following table describes the fields in this screen.

Table 54 NAT > DMZ Host

LABEL	DESCRIPTION
Default Server	Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT Port Forwarding** screen. Note: If you do not assign a **Default Server**, the P-2812HNU-51c discards all packets received for ports that are not specified in the **NAT Port Forwarding** screen.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.

8.6 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. The SIP ALG translates the P-2812HNU-51c's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if you enable the SIP ALG.

Use this screen to enable or disable the SIP (VoIP) ALG in the P-2812HNU-51c. To access this screen, click **NAT > ALG**.

Figure 87 NAT > ALG

Each field is described in the following table.

Table 55 NAT > ALG

LABEL	DESCRIPTION
Active SIP ALG	Select this check box to allow SIP sessions to pass through the P-2812HNU-51c. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol.
Apply	Click **Apply** to save your customized settings.

8.7 Technical Reference

The following section contains additional technical information about the P-2812HNU-51c features described in this chapter.

Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

Table 56 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161

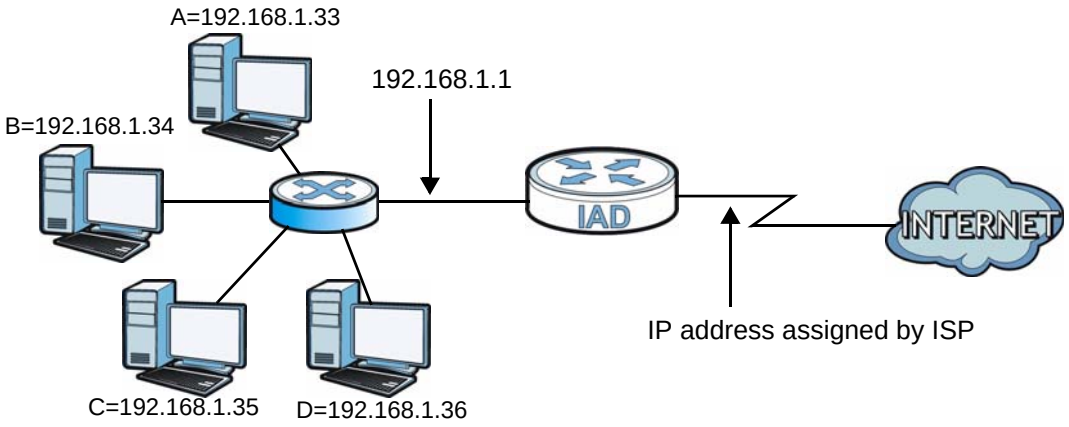
Table 56 Services and Port Numbers

SERVICES	PORT NUMBER
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 88 Multiple Servers Behind NAT Example



9

Voice

9.1 Overview

Use this chapter to:

- Connect an analog phone to the P-2812HNU-51c.
- Make phone calls over the Internet, as well as the regular phone network.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

9.1.1 What You Can Do in this Chapter

These screens allow you to configure your P-2812HNU-51c to make phone calls over the Internet and your regular phone line, and to set up the phones you connect to the P-2812HNU-51c.

- Use the **SIP Account** screen (Section 9.3 on page 197) to set up information about your SIP account, control which SIP accounts the phones connected to the P-2812HNU-51c use and configure audio settings such as volume levels for the phones connected to the ZyXEL Device.
- Use the **SIP Service Provider** screen (Section 9.4 on page 203) to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions, and dialing plan.
- Use the **Region** screen (Section 9.5 on page 211) to change settings that depend on the country you are in.
- Use the **Speed Dial** screen (Section 9.6 on page 212) to set up shortcuts for dialing frequently-used (VoIP) phone numbers.
- Use the **Call History Summary** screen (Section 9.8 on page 215) to view the summary list of received, dialed and missed calls.
- Use the **Outgoing Calls** screen (Section 9.8 on page 215) to view detailed information for each outgoing call you made.
- Use the **Incoming Calls** screen (Section 9.9 on page 216) to view detailed information for each incoming call from someone calling you.

You don't necessarily need to use all these screens to set up your account. In fact, if your service provider did not supply information on a particular field in a screen, it is usually best to leave it at its default setting.

9.1.2 What You Need to Know About VoIP

VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

SIP

SIP stands for Session Initiation Protocol. SIP is a signalling standard that lets one network device (like a computer or the P-2812HNU-51c) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your P-2812HNU-51c, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call.

SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the P-2812HNU-51c to use your SIP account to make calls, the P-2812HNU-51c is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you don't need a SIP account. It is possible for one SIP device (like the P-2812HNU-51c) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it tremendously impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup - figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

How to Find Out More

See Chapter 2 on page 33 for a tutorial showing how to set up these screens in an example scenario.

See Section 9.10 on page 216 for advanced technical information on SIP.

9.2 Before You Begin

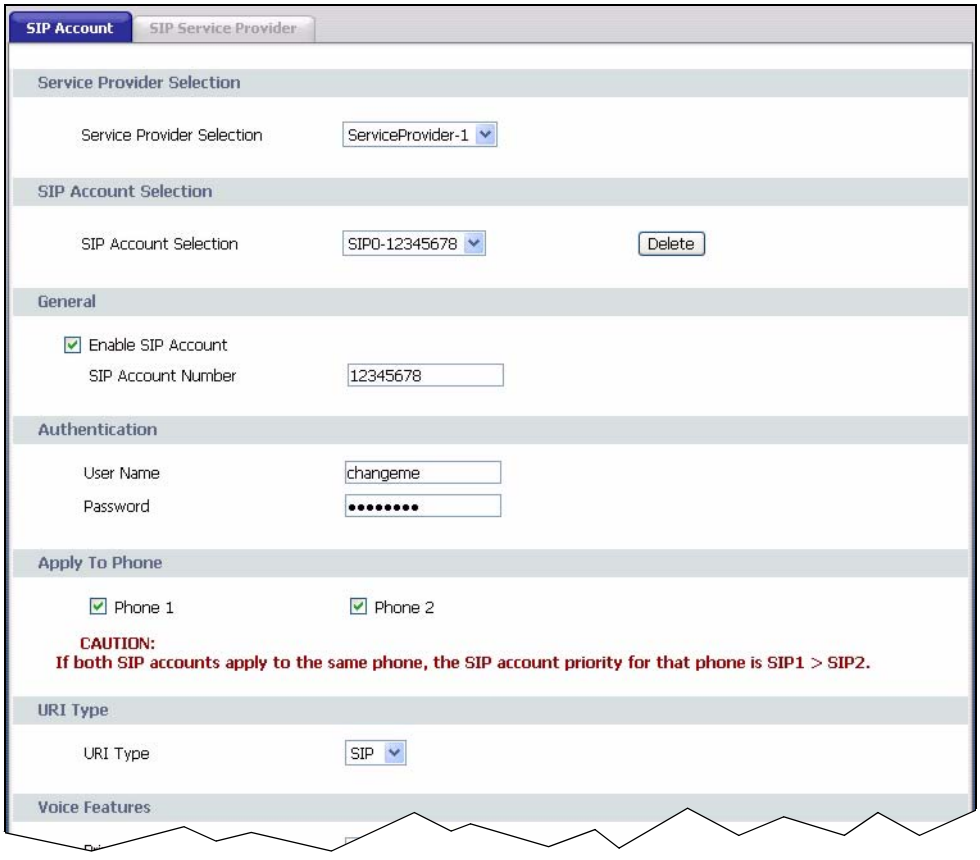
- Before you can use these screens, you need to have a VoIP account already set up. If you don't have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the P-2812HNU-51c.

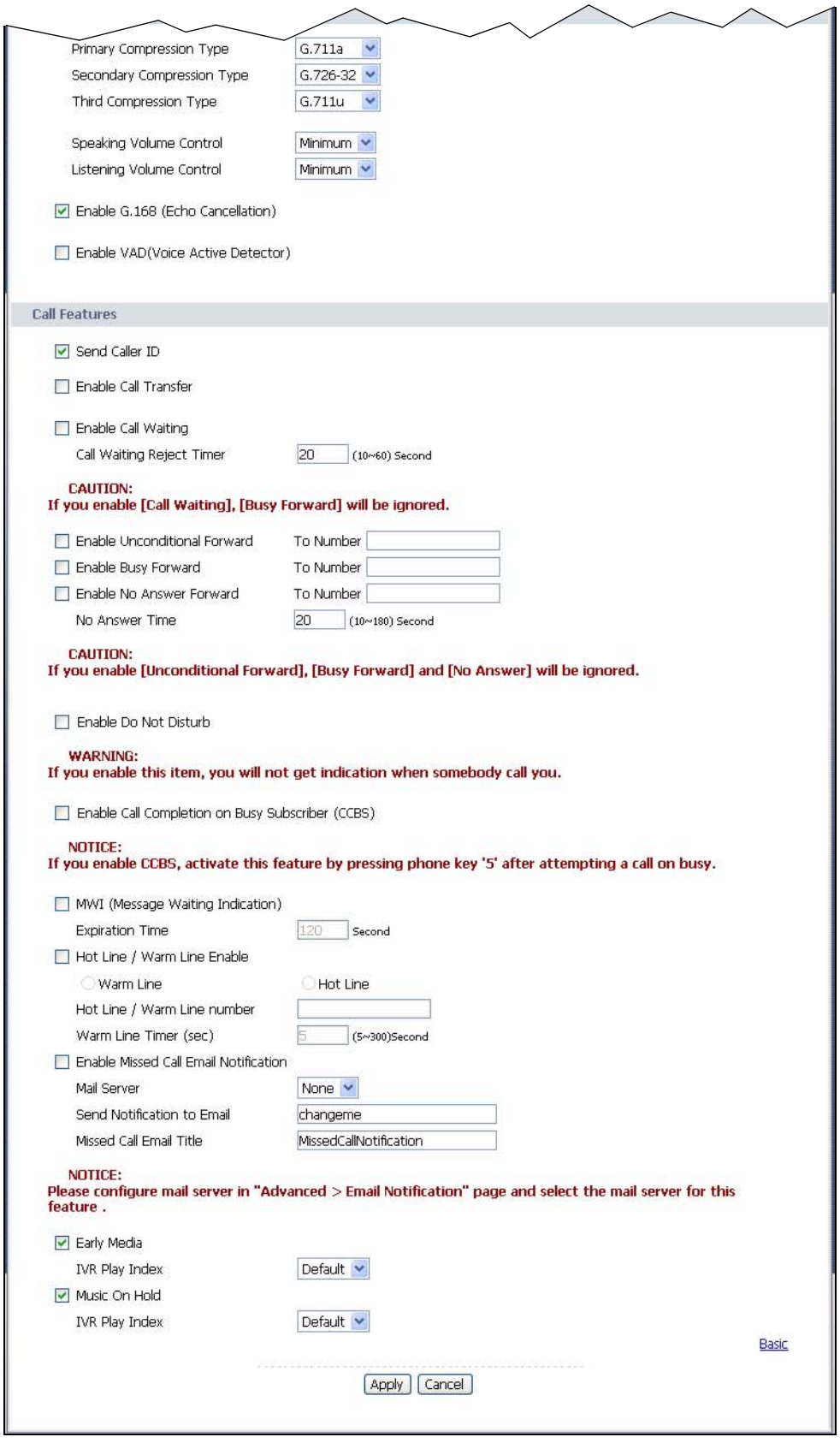
9.3 The SIP Settings Screen

The P-2812HNU-51c uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your P-2812HNU-51c to connect to your VoIP service provider.

Use this screen to maintain information about each SIP account. You can also enable and disable each SIP account. To access this screen, click **VoIP > SIP > SIP Account**.

Figure 89 VoIP > SIP > SIP Account




Primary Compression Type
G.711a
Secondary Compression Type
G.726-32
Third Compression Type
G.711u
Speaking Volume Control
Minimum
Listening Volume Control
Minimum
Enable G.168 (Echo Cancellation)
Enable VAD(Voice Active Detector)
Call Features
Send Caller ID
Enable Call Transfer
Enable Call Waiting
Call Waiting Reject Timer
20
(10~60) Second
CAUTION:
If you enable [Call Waiting], [Busy Forward] will be ignored.
Enable Unconditional Forward
To Number
Enable Busy Forward
To Number
Enable No Answer Forward
To Number
No Answer Time
20
(10~180) Second
CAUTION:
If you enable [Unconditional Forward], [Busy Forward] and [No Answer] will be ignored.
Enable Do Not Disturb
WARNING:
If you enable this item, you will not get indication when somebody call you.
Enable Call Completion on Busy Subscriber (CCBS)
NOTICE:
If you enable CCBS, activate this feature by pressing phone key '5' after attempting a call on busy.
MWI (Message Waiting Indication)
Expiration Time
120
Second
Hot Line / Warm Line Enable
Warm Line
Hot Line
Hot Line / Warm Line number
Warm Line Timer (sec)
5
(5~300)Second
Enable Missed Call Email Notification
Mail Server
None
Send Notification to Email
changeme
Missed Call Email Title
MissedCallNotification
NOTICE:
Please configure mail server in "Advanced > Email Notification" page and select the mail server for this feature .
Early Media
IVR Play Index
Default
Music On Hold
IVR Play Index
Default
Basic
Apply
Cancel

Each field is described in the following table.

Table 57 VoIP > SIP > SIP Account

LABEL	DESCRIPTION
Service Provider Selection	Select the SIP service provider profile you want to use for the SIP account you configure in this screen. If you change this field, the screen automatically refreshes.
SIP Account Selection	Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes. Select **ADD_NEW** to create a new SIP account on the P-2812HNU-51c.
Delete	Click this button to remove the SIP account selected in the **SIP Account Selection** field. This button is not available when you select **ADD_NEW** in the **SIP Account Selection** field.
General	
Enable SIP Account	Select this if you want the P-2812HNU-51c to use this account. Clear it if you do not want the P-2812HNU-51c to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
Authentication	
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters.
Apply To Phone	Select a phone port on which you want to make or receive phone calls for this SIP account. If you map a phone port to more than one SIP account, there is no way to distinguish between the SIP accounts when you receive phone calls. The P-2812HNU-51c uses the most recently registered SIP account first when you make an outgoing call. If a phone port is not mapped to a SIP account, you cannot receive or make any calls on the phone connected to this phone port.
Advanced/Basic	Click **Advanced** to display and edit more information for the SIP account. Click **Basic** to display and configure the basic SIP account settings.
URI Type	Select whether or not to include the SIP service domain name when the P-2812HNU-51c sends the SIP number. **SIP** - include the SIP service domain name. **TEL** - do not include the SIP service domain name.
Voice Features	

Table 57 VoIP > SIP > SIP Account (continued)

LABEL	DESCRIPTION
Primary Compression Type Secondary Compression Type Third Compression Type	Select the type of voice coder/decoder (codec) that you want the P-2812HNU-51c to use. G.711 provides high voice quality but requires more bandwidth (64 kbps). G.711 is the default codec used by phone companies and digital handsets. • **G.711a** is typically used in Europe. • **G.711u** is typically used in North America and Japan. **G.722** is a 7 KHz wideband voice codec that operates at 48, 56 and 64 kbps. By using a sample rate of 16 kHz, G.722 can provide higher fidelity and better audio quality than narrowband codecs like G.711, in which the voice signal is sampled at 8 KHz. **G.726** operates at **24** or **32** kbps. The P-2812HNU-51c must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec. Select the P-2812HNU-51c's first choice for voice coder/decoder. Select the P-2812HNU-51c's second choice for voice coder/decoder. Select **None** if you only want the P-2812HNU-51c to accept the first choice. Select the P-2812HNU-51c's third choice for voice coder/decoder. Select **None** if you only want the P-2812HNU-51c to accept the first or second choice.
Speaking Volume Control	Enter the loudness that the P-2812HNU-51c uses for speech that it sends to the peer device. **Minimum** is the quietest, and **Maximum** is the loudest.
Listening Volume Control	Enter the loudness that the P-2812HNU-51c uses for speech that it receives from the peer device. **Minimum** is the quietest, and **Maximum** is the loudest.
Enable G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Enable VAD (Voice Active Detector)	Select this if the P-2812HNU-51c should stop transmitting when you are not speaking. This reduces the bandwidth the P-2812HNU-51c uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Enable Call Transfer	Select this to enable call transfer on the P-2812HNU-51c. This allows you to transfer an incoming call (that you have answered) to another phone.
Enable Call Waiting	Select this to enable call waiting on the P-2812HNU-51c. This allows you to place a call on hold while you answer another incoming call on the same telephone number.

Table 57 VoIP > SIP > SIP Account (continued)

LABEL	DESCRIPTION
Call Waiting Reject Timer	Specify a time of seconds that the P-2812HNU-51c waits before rejecting the second call if you do not answer it.
Enable Unconditional Forward	Select this if you want the P-2812HNU-51c to forward all incoming calls to the specified phone number. Specify the phone number in the **To Number** field on the right.
Enable Busy Forward	Select this if you want the P-2812HNU-51c to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **To Number** field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Enable No Answer Forward	Select this if you want the P-2812HNU-51c to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Time**.) Specify the phone number in the **To Number** field on the right.
No Answer Time	This field is used by the **Active No Answer Forward** feature. Enter the number of seconds the P-2812HNU-51c should wait for you to answer an incoming call before it considers the call is unanswered.
Enable Do Not Disturb	Select this to set your phone to not ring when someone calls you.
Enable Call Completion on Busy Subscriber (CCBS)	When you make a phone call but hear a busy tone, Call Completion on Busy Subscriber (CCBS) allows you to enable auto-callback by pressing 5 and hanging up the phone. The P-2812HNU-51c then tries to call that phone number every minute since after you hang up the phone. When the called party becomes available within the CCBS timeout period (60 minutes by default), both phones ring. • If the called party's phone rings because of CCBS but no one answers the phone after 180 seconds, you will hear a busy tone. You can enable CCBS on the called number again. • If you manually call the number on which you have enabled CCBS before the CCBS timeout period expires, the P-2812HNU-51c disables CCBS on the called number. • If you call a second number before the first called number's CCBS timeout period expires, the P-2812HNU-51c stops calling the first number until you finish the second call. Select this option to activate CCBS on the P-2812HNU-51c.
MWI (Message Waiting Indication)	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
Expiration Time	Keep the default value for this field, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the P-2812HNU-51c subscribes to the service. Before this time passes, the P-2812HNU-51c automatically subscribes again.
Hot Line / Warm Line Enable	Select this to enable the hot line or warm line feature on the P-2812HNU-51c.

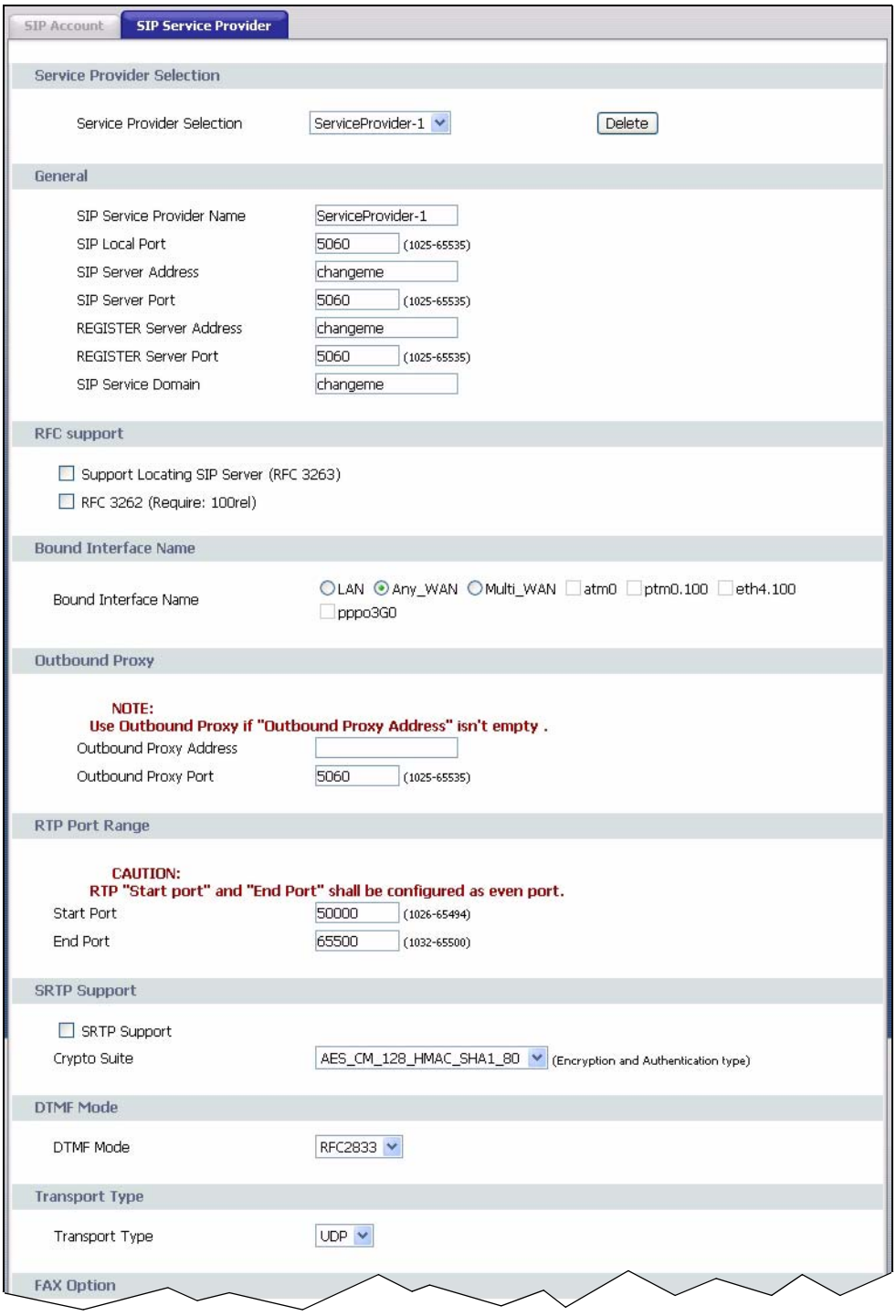
Table 57 VoIP > SIP > SIP Account (continued)

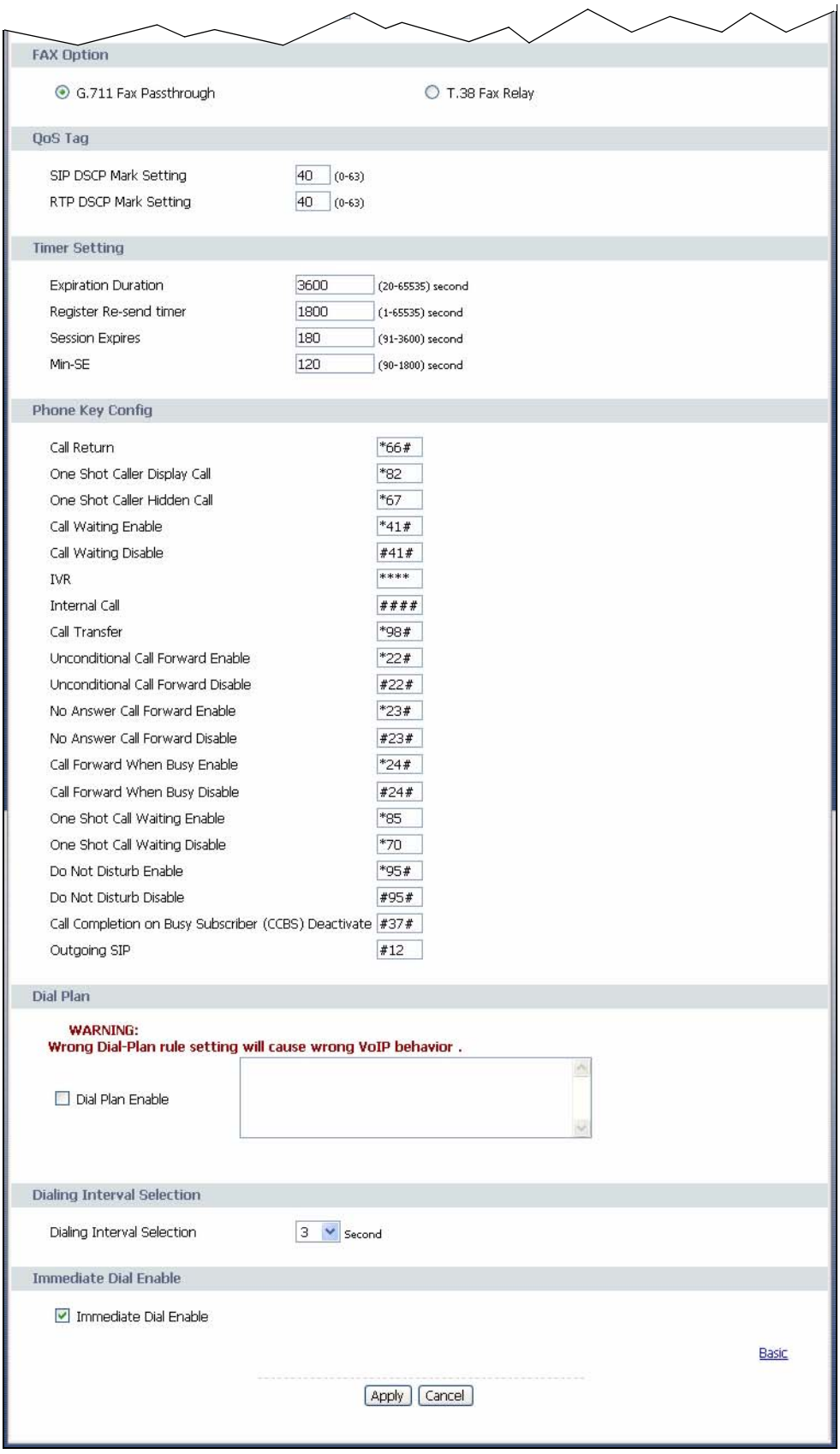
LABEL	DESCRIPTION
Warm Line	Select this to have the P-2812HNU-51c dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time.
Hot Line	Select this to have the P-2812HNU-51c dial the specified hot line number immediately when you pick up the telephone.
Hot Line / Warm Line number	Enter the number of the hot line or warm line that you want the P-2812HNU-51c to dial.
Warm Line Timer	Enter a number of seconds that the P-2812HNU-51c waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad.
Enable Missed Call Email Notification	Select this option to have the P-2812HNU-51c e-mail you a notification when there is a missed call.
Mail Server	Select a mail server for the e-mail address specified below. If you select **None** here, e-mail notifications will not be sent via e-mail. You must have configured a mail server already in the **Email Notification** screen.
Send Notification to Email	Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications will not be sent via e-mail.
Missed Call Email Title	Type a title that you want to be in the subject line of the e-mail notifications that the P-2812HNU-51c sends.
Early Media	Select this option if you want people to hear a customized recording when they call you.
IVR Play Index	Select the tone you want people to hear when they call you. This field is configurable only when you select **Early Media**. See Section 9.10 on page 216 for information on how to record these tones.
Music On Hold	Select this option to play a customized recording when you put people on hold.
IVR Play Index	Select the tone to play when you put someone on hold. This field is configurable only when you select **Music On Hold**. See Section 9.10 on page 216 for information on how to record these tones.
Apply	Click this to save your changes and to apply them to the P-2812HNU-51c.
Cancel	Click this to set every field in this screen to its last-saved value.

9.4 The SIP Service Provider Screen

Click **VoIP > SIP > SIP Service Provider** to open the **SIP Service Provider** screen. Use this screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions, and dialing plan.

Figure 90 VoIP > SIP > SIP Service Provider




FAX Option
G.711 Fax Passthrough
T.38 Fax Relay
QoS Tag
SIP DSCP Mark Setting 40 (0-63)
RTP DSCP Mark Setting 40 (0-63)
Timer Setting
Expiration Duration 3600 (20-65535) second
Register Re-send timer 1800 (1-65535) second
Session Expires 180 (91-3600) second
Min-SE 120 (90-1800) second
Phone Key Config
Call Return *66#
One Shot Caller Display Call *82
One Shot Caller Hidden Call *67
Call Waiting Enable *41#
Call Waiting Disable #41#
IVR ****
Internal Call ####
Call Transfer *98#
Unconditional Call Forward Enable *22#
Unconditional Call Forward Disable #22#
No Answer Call Forward Enable *23#
No Answer Call Forward Disable #23#
Call Forward When Busy Enable *24#
Call Forward When Busy Disable #24#
One Shot Call Waiting Enable *85
One Shot Call Waiting Disable *70
Do Not Disturb Enable *95#
Do Not Disturb Disable #95#
Call Completion on Busy Subscriber (CCBS) Deactivate #37#
Outgoing SIP #12
Dial Plan
WARNING:
Wrong Dial-Plan rule setting will cause wrong VoIP behavior .
Dial Plan Enable
Dialing Interval Selection
Dialing Interval Selection 3 Second
Immediate Dial Enable
Immediate Dial Enable
Basic
Apply
Cancel

Each field is described in the following table.

Table 58 VoIP > SIP > SIP Service Provider

LABEL	DESCRIPTION
Service Provider Selection	Select the SIP service provider profile you want to see in this screen. If you change this field, the screen automatically refreshes. Select **ADD_NEW** to create a new SIP service provider profile on the P-2812HNU-51c.
Delete	Click this button to remove the SIP service provider profile selected in the **Service Provider Selection** field. This button is not available when you select **ADD_NEW** in the **Service Provider Selection**.
General	
SIP Service Provider Name	Enter a descriptive name of up to 63 printable characters for this SIP service provider profile. Spaces are not allowed.
SIP Local Port	Enter the P-2812HNU-51c's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
RFC support	
Support Locating SIP Server (RFC 3263)	Select this option to have the P-2812HNU-51c use DNS procedures to resolve the SIP domain and find the SIP server's IP address, port number and supported transport protocol(s). The P-2812HNU-51c first uses DNS Name Authority Pointer (NAPTR) records to determine the transport protocols supported by the SIP server. It then performs DNS Service (SRV) query to determine the port number for the protocol. The P-2812HNU-51c resolves the SIP server's IP address by a standard DNS address record lookup. The **SIP Server Port** and **REGISTER Server Port** fields are grayed out and not applicable and the **Transport Type** can also be set to **AUTO** if you select this option.

Table 58 VoIP > SIP > SIP Service Provider (continued)

LABEL	DESCRIPTION
RFC 3262	RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Select this to have the P-2812HNU-51c include a SIP Require/ Supported header field with the option tag 100rel in all INVITE requests. When the P-2812HNU-51c receives a SIP response message indicating that the phone it called is ringing, the P-2812HNU-51c sends a PRACK message to have both sides confirm the message is received. If you select this option, the peer device should also support the option tag 100rel to send provisional responses reliably.
Bound Interface Name	
Bound Interface Name	If you select **LAN** or **Any_WAN**, the P-2812HNU-51c automatically activates the VoIP service when any LAN or WAN connection is up. If you select **Multi_WAN**, you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up.
Outbound Proxy	
Outbound Proxy Address	Enter the IP address or domain name of the SIP outbound proxy server if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the P-2812HNU-51c to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the P-2812HNU-51c to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Outbound Proxy Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
RTP Port Range	
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.

Table 58 VoIP > SIP > SIP Service Provider (continued)

LABEL	DESCRIPTION
SRTP Support	When you make a VoIP call using SIP, the Real-time Transport Protocol (RTP) is used to handle voice data transfer. The Secure Real-time Transport Protocol (SRTP) is a security profile of RTP. It is designed to provide encryption and authentication for the RTP data in both unicast and multicast applications. SRTP uses the Advanced Encryption Standard (AES) cipher for data encryption. The P-2812HNU-51c supports encryption using AES with a 128-bit key. To protect data integrity, SRTP uses a Hash-based Message Authentication Code (HMAC) calculation with Secure Hash Algorithm (SHA)-1 to authenticate data. HMAC SHA-1 produces a 80 or 32-bit authentication tag that is appended to the packet. Both the caller and callee should use the same algorithms to establish an SRTP session.
SRTP Support	Select this option to enable SRTP on the P-2812HNU-51c.
Crypto Suite	Select the encryption and authentication algorithm set used by the P-2812HNU-51c to set up an SRTP media session with the peer device. Select **AES_CM_128_HMAC_SHA1_80** or **AES_CM_128_HMAC_SHA1_32** to enable both data encryption and authentication for voice data. Select **AES_CM_128_NULL** to use 128-bit data encryption but disable data authentication. Select **NULL_CIPHER_HMAC_SHA1_80** to disable encryption but require authentication using the default 80-bit tag.
DTMF Mode	
DTMF Mode	Control how the P-2812HNU-51c handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC2833** - send the DTMF tones in RTP packets. **InBand** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. **SIPInfo** - send the DTMF tones in SIP messages.
Transport Type	
Transport Type	Select the transport layer protocol (**TCP**, **UDP** or **TLS**) used for SIP. **AUTO** is available when you select the **Support Locating SIP Server** option. If you select **AUTO** here, the P-2812HNU-51c sends a DNS Name Authority Pointer (NAPTR) query to locate the SIP server and get the supported transport layer protocol(s).
FAX Option	This field controls how the P-2812HNU-51c handles fax messages.
G.711 Fax Passthrough	Select this if the P-2812HNU-51c should use G.711 to send fax messages. The peer devices must also use G.711.

Table 58 VoIP > SIP > SIP Service Provider (continued)

LABEL	DESCRIPTION
T.38 Fax Relay	Select this if the P-2812HNU-51c should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
QoS Tag	
SIP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for SIP voice transmissions. The P-2812HNU-51c creates Class of Service (CoS) priority tags with this number to voice traffic that it transmits.
RTP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The P-2812HNU-51c creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The P-2812HNU-51c automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the P-2812HNU-51c waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the P-2812HNU-51c lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the P-2812HNU-51c lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the P-2812HNU-51c accepts.
Phone Key Config	
Call Return	Specify the key combinations that you can enter to place a call to the last number that called you.
One Shot Caller Display Call	Specify the key combinations that you can enter to activate caller ID for the next call only.
One Shot Caller Hidden Call	Specify the key combinations that you can enter to deactivate caller ID for the next call only.
Call Waiting Enable	Specify the key combinations that you can enter to put a call on hold when you are answering another.
Call Waiting Disable	Specify the key combinations that you can enter to turn the call waiting function off.
IVR	Specify the key combinations that you can enter to set up Interactive Voice Response (IVR). IVR allows you to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold).
Internal Call	Specify the key combinations that you can enter to call the phone(s) connected to the P-2812HNU-51c.
Call Transfer	Specify the key combinations that you can enter to transfer a call to another phone.

Table 58 VoIP > SIP > SIP Service Provider (continued)

LABEL	DESCRIPTION
Unconditional Call Forward Enable	Specify the key combinations that you can enter to forward all incoming calls to the phone number you specified in the **SIP > SIP Account** screen.
Unconditional Call Forward Disable	Specify the key combinations that you can enter to turn the unconditional call forward function off.
No Answer Call Forward Enable	Specify the key combinations that you can enter to forward incoming calls to the phone number you specified in the **SIP > SIP Account** screen if the calls are unanswered.
No Answer Call Forward Disable	Specify the key combinations that you can enter to turn the no answer call forward function off.
Call Forward When Busy Enable	Specify the key combinations that you can enter to forward incoming calls to the phone number you specified in the **SIP > SIP Account** screen if the phone port is busy.
Call Forward When Busy Disable	Specify the key combinations that you can enter to turn the busy forward function off.
One Shot Call Waiting Enable	Specify the key combinations that you can enter to activate call waiting on the next call only.
One Shot Call Waiting Disable	Specify the key combinations that you can enter to deactivate call waiting on the next call only.
Do Not Disturb Enable	Specify the key combinations that you can enter to set your phone not to ring when someone calls you.
Do Not Disturb Disable	Specify the key combinations that you can enter to turn this function off.
Call Completion on Busy Subscriber (CCBS) Deactivate	Specify the key combinations that you can enter to disable CCBS on a call.
Outgoing SIP	Specify the key combinations that you can enter to select the SIP account that you use to make outgoing calls. If you enter #12(by default)<SIP account index number>#<the phone number you want to call>, #1201#12345678 for example, the P-2812HNU-51c uses the first SIP account to call 12345678.
Dial Plan	
Dial Plan Enable	Select this to activate the dial plan rules you specify in the text box provided. See Section 9.4.1 on page 210 for how to set up a rule.
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the P-2812HNU-51c should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. If you select **Immediate Dial Enable**, you can press the pound key (#) to tell the P-2812HNU-51c to make the phone call immediately, regardless of this setting.

Table 58 VoIP > SIP > SIP Service Provider (continued)

LABEL	DESCRIPTION
Immediate Dial Enable	
Immediate Dial Enable	Select this if you want to use the pound key (#) to tell the P-2812HNU-51c to make the phone call immediately, instead of waiting the number of seconds you selected in the **Dialing Interval Selection** field. If you select this, dial the phone number, and then press the pound key. The P-2812HNU-51c makes the call immediately, instead of waiting. You can still wait, if you want.
Apply	Click this to save your changes and to apply them to the P-2812HNU-51c.
Cancel	Click this to set every field in this screen to its last-saved value.

9.4.1 Dial Plan Rules

A dial plan defines the dialing patterns, such as the length and range of the digits for a telephone number. It also includes country codes, access codes, area codes, local numbers, long distance numbers or international call prefixes. For example, the dial plan ([2-9]xxxxxx) does not allow a local number which begins with 1 or 0.

Without a dial plan, users have to manually enter the whole callee's number and wait for the specified dialing interval to time out or press a terminator key (usually the pound key on the phone keypad) before the P-2812HNU-51c makes the call.

The P-2812HNU-51c initializes a call when the dialed number matches any one of the rules in the dial plan. Dial plan rules follow these conventions:

- The collection of rules is in parentheses ().
- Rules are separated by the | (bar) symbol.
- "x" stands for a wildcard and can be any digit from 0 to 9.
- A subset of keys is in a square bracket []. Ranges are allowed.

  For example, [359] means a number matching this rule can be 3, 5 or 9. [26-8*] means a number matching this rule can be 2, 6, 7, 8 or *.
- The dot "." appended to a digit allows the digit to be ignored or repeated multiple times. Any digit (0~9, *, #) after the dot will be ignored.

  For example, (01.) means a number matching this rule can be 0, 01, 0111, 01111, and so on.

- <dialed-number:translated-number> indicates the number after the colon replaces the number before the colon in an angle bracket <>. For example,

  (<:1212> xxxxxxx) means the P-2812HNU-51c automatically prefixes the translated-number “1212” to the number you dialed before making the call. This can be used for local calls in the US.

  (<9:> xxx xxxxxxx) means the P-2812HNU-51c automatically removes the specified prefix “9” from the number you dialed before making the call. This is always used for making outside calls from an office.

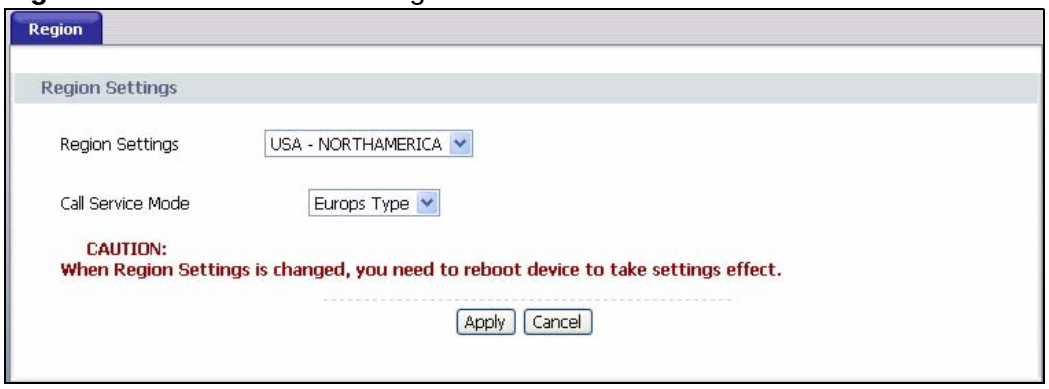
  (xx<123:456>xxxx) means the P-2812HNU-51c automatically translates “123” to “456” in the number you dialed before making the call.
- Calls with a number followed by the exclamation mark “!” will be dropped.
- Calls with a number followed by the termination character “@” will be made immediately. Any digit (0~9, *, #) after the @ character will be ignored.

In this example dial plan (0 | [49]11 | 1 [2-9]xx xxxxxxx | 1 947 xxxxxxx !), you can dial “0” to call the local operator, call 411 or 911, or make a long distance call with an area code starting from 2 to 9 in the US. The calls with the area code 947 will be dropped.

9.5 The Phone Region Screen

Use this screen to maintain settings that depend on which region of the world the P-2812HNU-51c is in. To access this screen, click **VoIP > Phone > Region**.

Figure 91 VoIP > Phone > Region



Each field is described in the following table.

Table 59 VoIP > Phone > Region

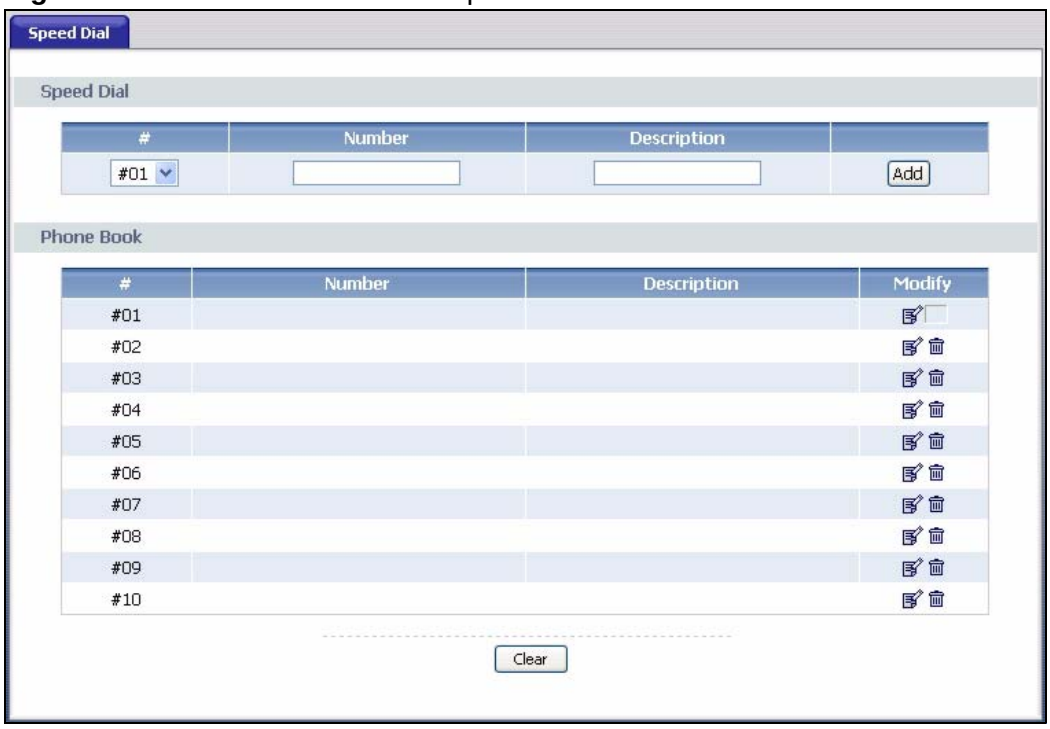
LABEL	DESCRIPTION
Region Settings	Select the place in which the P-2812HNU-51c is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. **Europe Type** - use supplementary phone services in European mode **USA Type** - use supplementary phone services American mode You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the P-2812HNU-51c.
Cancel	Click this to set every field in this screen to its last-saved value.

9.6 The Speed Dial Screen

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut

(the speed dial number, #01 for example) on your phone's keypad to call the phone number.

Figure 92 VoIP > Phone Book > Speed Dial



Each field is described in the following table.

Table 60 VoIP > Phone Book > Speed Dial

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
#	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the P-2812HNU-51c to call when you dial the speed-dial number.
Description	Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Add	Click this to use the information in the **Speed Dial** section to update the **Phone Book** section.
Phone Book	Use this section to look at all the speed-dial entries and to erase them.
#	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the P-2812HNU-51c calls when you dial the speed-dial number.
Description	This field displays the name of the party you call when you dial the speed-dial number.

Table 60 VoIP > Phone Book > Speed Dial

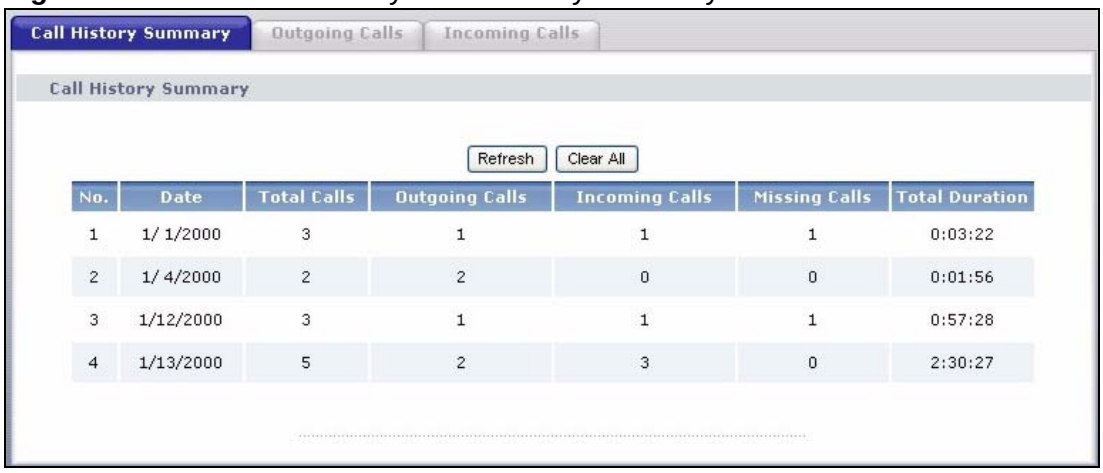
LABEL	DESCRIPTION
Modify	Use this field to edit or erase the speed-dial entry. Click the **Edit** icon to copy the information for this speed-dial entry into the **Speed Dial** section, where you can change it. Click the **Remove** icon to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.

9.7 Call History Summary Screen

The P-2812HNU-51c logs calls from or to your SIP numbers. This screen allows you to view the summary of received, dialed and missed calls.

Click **VoIP > Call History > Call History Summary**. The following screen displays.

Figure 93 VoIP > Call History > Call History Summary



Each field is described in the following table.

Table 61 VoIP > Call History > Call History Summary

LABEL	DESCRIPTION
Refresh	Click this button to renew the call history list.
Clear All	Click this button to remove all entries from the call history list.
No.	This is a read-only index number.
Date	This is the date when the calls were made.
Total Calls	This displays the total number of calls from or to your SIP numbers that day.
Outgoing Calls	This displays how many calls originated from you that day.
Incoming Calls	This displays how many calls you received that day.

Table 61 VoIP > Call History > Call History Summary

LABEL	DESCRIPTION
Missing Calls	This displays how many incoming calls were not answered that day.
Total Duration	This displays how long all calls lasted that day.

9.8 Outgoing Calls Screen

Use this screen to see detailed information for each outgoing call you made.

Click **VoIP > Call History > Outgoing Calls**. The following screen displays.

Figure 94 VoIP > Call History > Outgoing Calls

Each field is described in the following table.

Table 62 VoIP > Call History > Outgoing Calls

LABEL	DESCRIPTION
Refresh	Click this button to renew the dialed call list.
Clear All	Click this button to remove all entries from the dialed call list.
No.	This is a read-only index number.
time	This is the date and time when the call was made.
phone port	This is the phone port on which you made the call.
phone number	This is the SIP number you called.
duration	This displays how long the call lasted.

9.9 Incoming Calls Screen

Use this screen to see detailed information for each incoming call from someone calling you.

Click **VoIP > Call History > Incoming Calls**. The following screen displays.

Figure 95 VoIP > Call History > Incoming Calls

Each field is described in the following table.

Table 63 VoIP > Call History > Incoming Calls

LABEL	DESCRIPTION
Refresh	Click this button to renew the received call list.
Clear All	Click this button to remove all entries from the received call list.
No.	This is a read-only index number.
time	This is the date and time when the call was made.
phone port	This is the phone port on which you received the call. **Missed** means the call was unanswered.
phone number	This is the SIP number that called you.
duration	This displays how long the call lasted.

9.10 Technical Reference

This section contains background material relevant to the **VoIP** screens.

VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

SIP Registration

Each P-2812HNU-51c is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the P-2812HNU-51c). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The P-2812HNU-51c attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the P-2812HNU-51c attempts to register the port immediately.

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC3261, "SIP: Session Initiation Protocol").

SIP Servers

SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

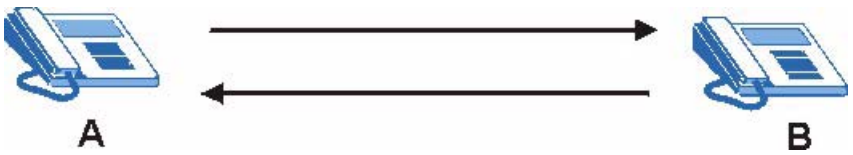
When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server

protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP user agent to receive the call.

Figure 96 SIP User Agent



SIP Proxy Server

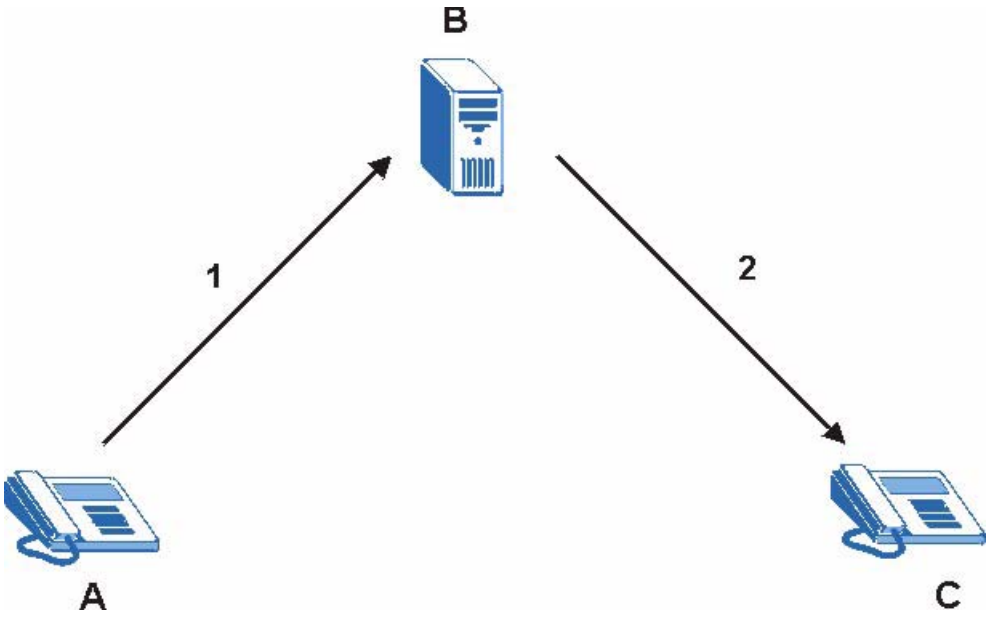
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device C.

1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server (**B**).

2 The SIP proxy server forwards the call invitation to **C**.

Figure 97 SIP Proxy Server



SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests

to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

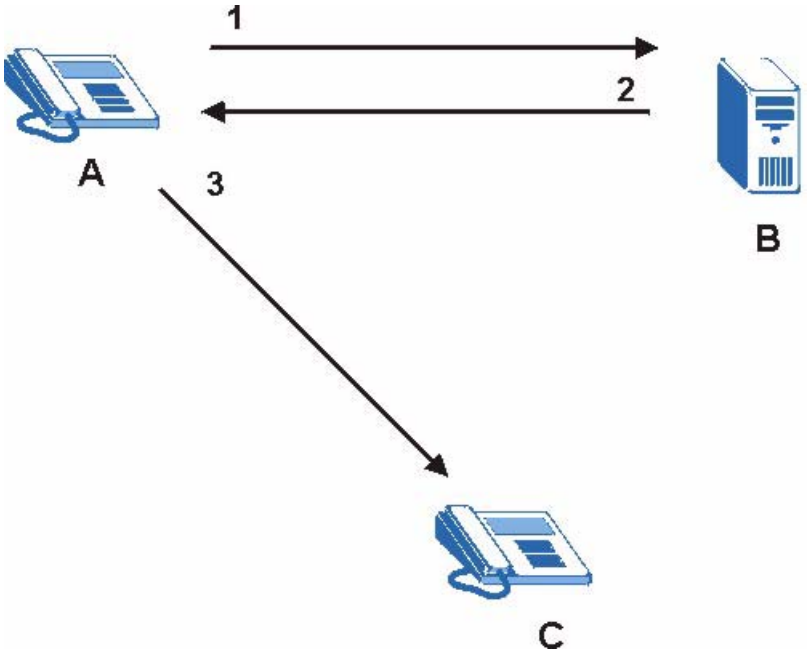
In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 Client device **A** sends a call invitation for **C** to the SIP redirect server (**B**).

2 The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).

3 Client device **A** then sends the call invitation to client device **C**.

Figure 98 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 64 SIP Call Progression

A		B
1. INVITE	→	
	←	2. Ringing
	←	3. OK
4. ACK	→	
	5.Dialogue (voice traffic)	
6. BYE	→	
	←	7. OK

1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.

2 **B** sends a response indicating that the telephone is ringing.

3 **B** sends an OK response after the call is answered.

4 **A** then sends an ACK message to acknowledge that **B** has answered the call.

5 Now **A** and **B** exchange voice media (talk).

6 After talking, **A** hangs up and sends a BYE request.

7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

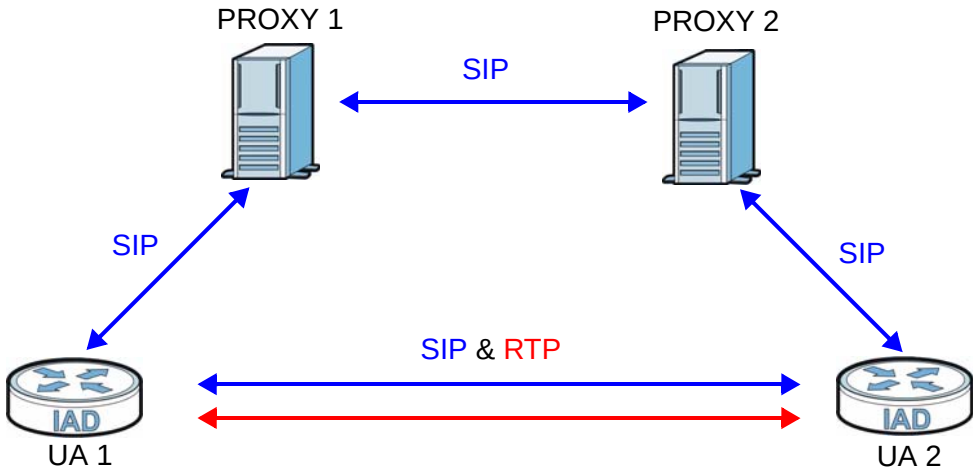
SIP Call Progression Through Proxy Servers

Usually, the SIP UAC sets up a phone call by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

The response to the request goes to all the proxy servers through which the request passed, in reverse sequence. Once the session is set up, session traffic is sent between the UAs directly, bypassing all the proxy servers in between.

The following figure shows the SIP and session traffic flow between the user agents (**UA 1** and **UA 2**) and the proxy servers (this example shows two proxy servers, **PROXY 1** and **PROXY 2**).

Figure 99 SIP Call Through Proxy Servers



The following table shows the SIP call progression.

Table 65 SIP Call Progression

UA 1		PROXY 1		PROXY 2		UA 2
Invite	→					
		Invite	→			
		100 Trying	←	Invite	→	
				100 Trying	←	
						180 Ringing
				180 Ringing	←	
		180 Ringing	←			
						200 OK
				200 OK	←	
		200 OK	←			
ACK	→					
RTP	↔					RTP
						BYE
200 OK	→					

1 **User Agent 1** sends a SIP INVITE request to **Proxy 1**. This message is an invitation to **User Agent 2** to participate in a SIP telephone call. **Proxy 1** sends a response indicating that it is trying to complete the request.

2 **Proxy 1** sends a SIP INVITE request to **Proxy 2**. **Proxy 2** sends a response indicating that it is trying to complete the request.

3 **Proxy 2** sends a SIP INVITE request to **User Agent 2**.

4 **User Agent 2** sends a response back to **Proxy 2** indicating that the phone is ringing. The response is relayed back to **User Agent 1** via **Proxy 1**.

5 **User Agent 2** sends an OK response to **Proxy 2** after the call is answered. This is also relayed back to **User Agent 1** via **Proxy 1**.

6 **User Agent 1** and **User Agent 2** exchange RTP packets containing voice data directly, without involving the proxies.

7 When **User Agent 2** hangs up, he sends a BYE request.

8 **User Agent 1** replies with an OK response confirming receipt of the BYE request, and the call is terminated.

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The P-2812HNU-51c supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the P-2812HNU-51c reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

Comfort Noise Generation

When using VAD, the P-2812HNU-51c generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the P-2812HNU-51c. The P-2812HNU-51c allows you to record custom tones for the **Early Media** and **Music On Hold** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 66 Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	900 seconds for all custom tones combined
Maximum Time per Individual Tone	180 seconds
Total Number of Tones Recordable	5 You can record up to 5 different custom tones but the total time must be 900 seconds or less.

Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

1 Pick up the phone and press "*****" on your phone's keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1101~1105 on your phone followed by the "#" key.

3 Play your desired music or voice recording into the receiver's mouthpiece. Press the "#" key.

4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Listening to Custom Tones

Do the following to listen to a custom tone:

1 Pick up the phone and press "*****" on your phone's keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1201~1208 followed by the "#" key to listen to the tone.

3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Deleting Custom Tones

Do the following to delete a custom tone:

1 Pick up the phone and press "*****" on your phone's keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1301~1308 followed by the "#" key to delete the tone of your choice. Press 14 followed by the "#" key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

9.10.1 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the P-2812HNU-51c) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

DiffServ

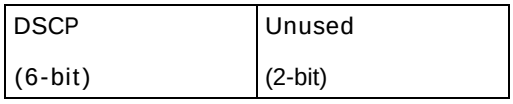
DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[3]

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

Figure 100 DiffServ: Differentiated Service Field



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

3. The P-2812HNU-51c does not support DiffServ at the time of writing.

9.10.2 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer. are generally available from your VoIP service provider. The P-2812HNU-51c supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Call Park and Pickup
- Do not Disturb

Note: To take full advantage of the supplementary phone services available through the P-2812HNU-51c's phone ports, you may need to subscribe to the services from your VoIP service provider.

9.10.2.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the P-2812HNU-51c.

You can invoke all the supplementary services by using the flash key.

9.10.2.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 67 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press “0”.

- Disconnect the first call and answer the second call.

  Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.

- Put the first call on hold and answer the second call.

  Press the flash key and then “2”.

European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call.
3. After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key and press “3” to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

9.10.2.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 68 USA Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call.
3. After you hear the ring signal or the second party answers it, hang up the phone.

USA Three-Way Conference

Use the following steps to make three-way conference calls.

1 When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.

2 Dial a phone number directly to make another call (to party B).

3 When party B answers the second call, press the flash key to create a three-way conversation.

4 Hang up the phone to drop the connection.

5 If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.

6 If you want to go back to the three-way conversation, press the flash key again.

7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

9.10.2.4 Phone Functions Summary

The following table shows the key combinations you can enter on your phone's keypad to use certain features.

Table 69 Phone Functions Summary

ACTION	FUNCTION	DESCRIPTION
*98#	Call transfer	Transfer a call to another phone. See Section 9.10.2.2 on page 227 (Europe type) and Section 9.10.2.3 on page 229 (USA type).
*66#	Call return	Place a call to the last person who called you.
*95#	Enable Do Not Disturb	Use these to set your phone not to ring when someone calls you, or to turn this function off.
#95#	Disable Do Not Disturb	
*41#	Enable Call Waiting	Use these to allow you to put a call on hold when you are answering another, or to turn this function off.
#41#	Disable Call Waiting	
****	IVR	Use these to set up Interactive Voice Response (IVR). IVR allows you to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold).
####	Internal Call	Call the phone(s) connected to the P-2812HNU-51c.
*82	One Shot Caller Display Call	Activate or deactivate caller ID for the next call only.
*67	One Shot Caller Hidden Call	

10

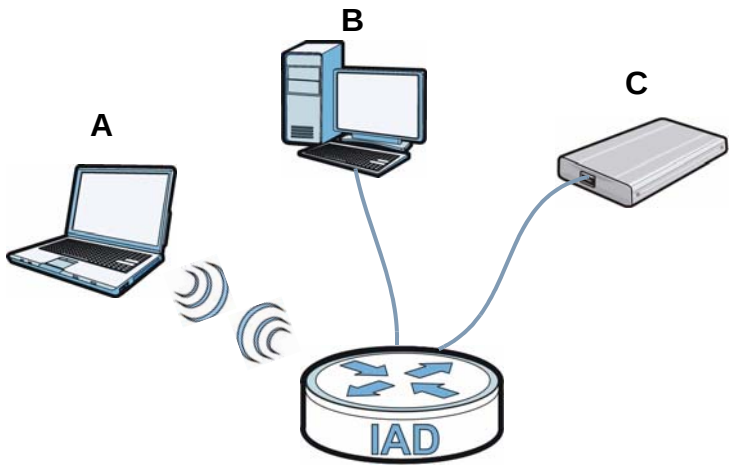
File Sharing

10.1 Overview

Share files on a USB memory stick or hard drive connected to your P-2812HNU-51c with users on your network.

The following figure is an overview of the P-2812HNU-51c's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the P-2812HNU-51c.

Figure 101 File Sharing Overview



- See Section 10.1.2 on page 234 for an explanation of file-sharing terms.
- See Section 10.2.1 on page 237 for file-sharing examples.

10.1.1 What You Can Do in this chapter

The **File Sharing** screen lets you enable file-sharing server on the P-2812HNU-51c and configure the workgroup name (Section 10.2 on page 236).

10.1.2 What You Need to Know

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the P-2812HNU-51c is given a folder, called a “share”. If a USB hard drive connected to the P-2812HNU-51c has more than one partition, then each partition will be allocated a share. You can also configure a “share” to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file-sharing feature on your P-2812HNU-51c supports File Allocation Table (FAT) and FAT32 file systems.

Windows/CIFS

Common Internet File System (CIFS) is a standard protocol supported by most operating systems in order to share files across the network.

CIFS runs over TCP/IP but uses the SMB (Server Message Block) protocol found in Microsoft Windows for file and printer access; therefore, CIFS will allow all applications, not just Web browsers, to open and share files across the Internet.

The P-2812HNU-51c uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the P-2812HNU-51c. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

NFS

Network File System (NFS) is a protocol most commonly used on Unix-like systems in order to share files across the network.

Samba

SMB is a client-server protocol used by Microsoft Windows systems for sharing files, printers, and so on.

Samba is a free SMB server that runs on most Unix and Unix-like systems. It provides an implementation of an SMB client and server for use with non-Microsoft operating systems.

File Transfer Protocol

This is a method of transferring data from one computer to another over a network such as the Internet.

10.1.3 Before You Begin

Make sure the P-2812HNU-51c is connected to your network and turned on.

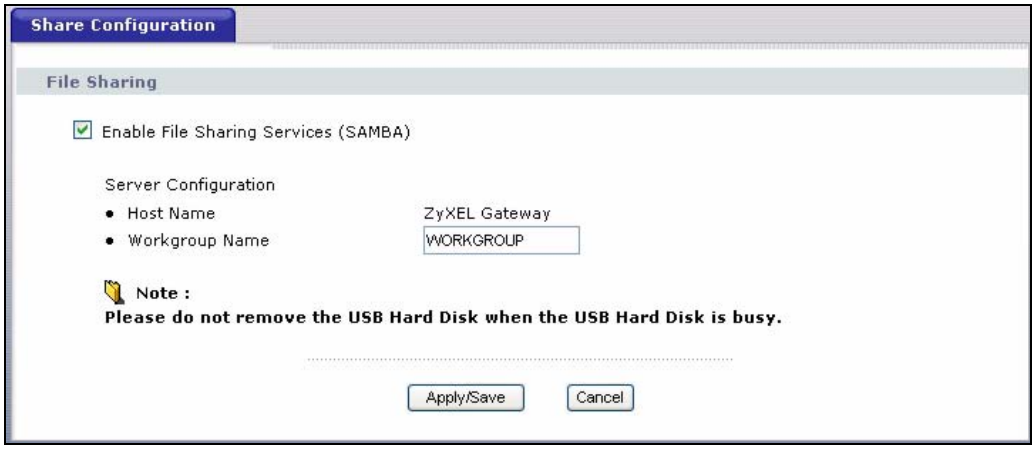
1. Connect the USB device to one of the P-2812HNU-51c's USB ports. Make sure the P-2812HNU-51c is connected to your network.
2. The P-2812HNU-51c detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by P-2812HNU-51c, see the troubleshooting for suggestions.

10.2 The File Sharing Screen

Use this screen to set up file sharing via the P-2812HNU-51c. To access this screen, click **USB Services > File Sharing**.

Figure 102 USB Services > File Sharing



Each field is described in the following table.

Table 70 USB Services > File Sharing

LABEL	DESCRIPTION
Enable File Sharing Services	Select this to enable file sharing through the P-2812HNU-51c.
Server Configuration	
Host Name	This displays the P-2812HNU-51c system name.
Workgroup Name	You can add the P-2812HNU-51c to an existing or a new workgroup on your network. Enter the name of the workgroup which your P-2812HNU-51c automatically joins. You can set the P-2812HNU-51c's workgroup name to be exactly the same as the workgroup name to which your computer belongs to. Note: The P-2812HNU-51c will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.
Apply	Click this to save your changes to the P-2812HNU-51c.
Reset	Click this to set every field in this screen to its last-saved value.

10.2.1 Example of Accessing Your Shared Files From a Computer

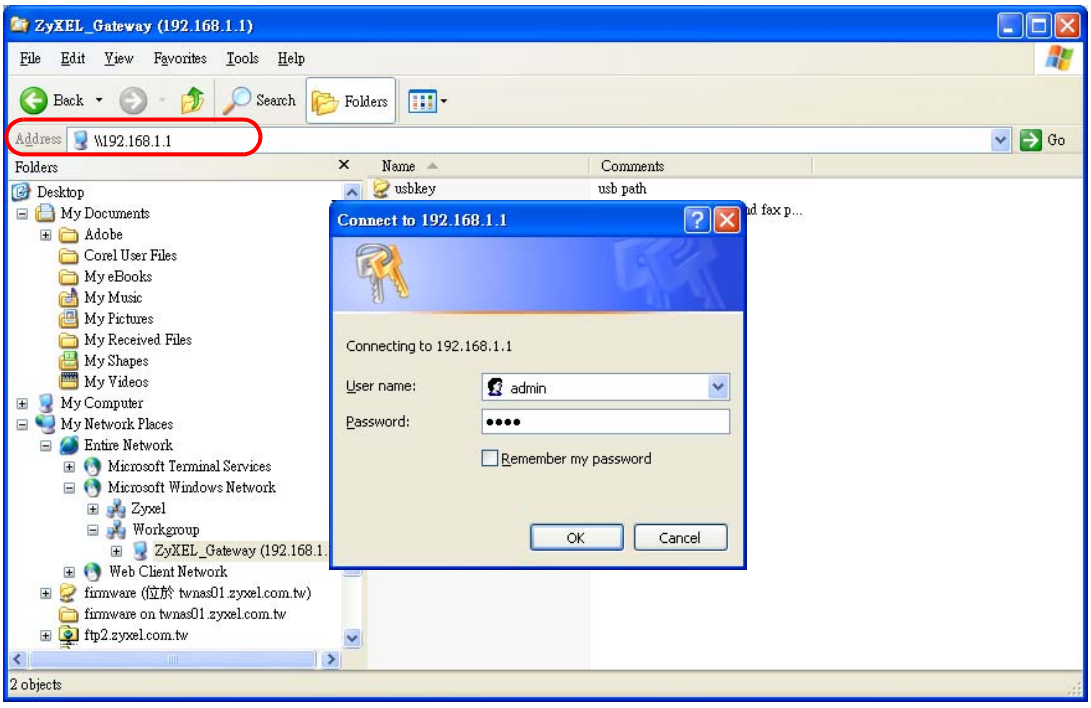
You can use Windows Explorer to access the file storage devices connected to the P-2812HNU-51c.

Note: The example in this User's Guide shows you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

1 Open Windows Explorer to share files in the attached USB device using Windows Explorer browser.

2 In Windows Explorer's Address bar type a double backslash "\\" followed by the IP address of the P-2812HNU-51c (the default IP address of the P-2812HNU-51c is 192.168.1.1) and press [ENTER]. A screen asking for password authentication appears. Type the user name and password you use to access the system and click **OK**. (The default system user name is **admin** or **user** and the default system password is **1234** or **user**.)

Figure 103 File Sharing via Windows Explorer



Note: Once you log in to the file share via your P-2812HNU-51c, you do not have to log in again unless you restart your computer.

11

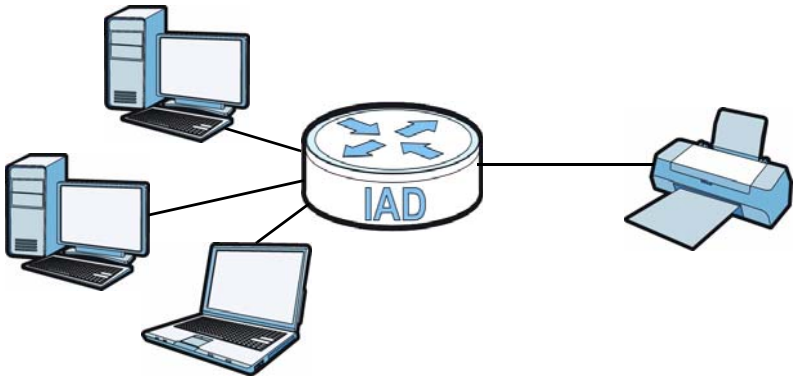
Sharing a USB Printer

This chapter describes how you can share a USB printer via your P-2812HNU-51c.

11.1 Overview

The P-2812HNU-51c allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the P-2812HNU-51c and then allowing the computers connected to your network to communicate with the print server (P-2812HNU-51c) using the Internet Printing Protocol.

Figure 104 Sharing a USB Printer



11.1.1 What You Can Do in this chapter

- The **Print Server** screen lets you enable the print server on the P-2812HNU-51c and get the model name of the associated printer. (Section 11.4 on page 241).
- This chapter also shows you examples of adding a new network printer using Windows (Section 11.5 on page 242) and adding a new network printer using Macintosh OS X (Section 11.6 on page 245)

11.2 What You Need to Know

Print Server

This is a computer or other device which manages one or more printers, and which sends print jobs to each printer from the computer itself or other devices.

Operating System

An operating system (OS) is the interface which helps you manage a computer. Common examples are Microsoft Windows, Mac OS or Linux.

Port

A port maps a network service such as http to a process running on your computer, such as a process run by your web browser. When traffic from the Internet is received on your computer, the port number is used to identify which process running on your computer it is intended for.

Internet Printing Protocol

The Internet Printing Protocol (IPP) uses TCP and UDP with port 631. It can run locally or over the Internet on top of HTTP. It allows users to send print jobs to a printer, cancel a previous print job, and know the status of the printer and print jobs.

Supported OSs

The following OSs support P-2812HNU-51c's printer sharing feature.

- Microsoft Windows 2000, Windows XP, Windows 7, Windows Vista or Macintosh OS X and later versions.

11.3 Before You Begin

To configure the print server you need the following:

- Your P-2812HNU-51c must be connected to your computer and any other devices on your network. The USB printer must be connected to your P-2812HNU-51c.
- The computers on your network must have the printer software already installed before they can use the printer. Follow your printer manufacturers instructions on how to install the printer software on your computer.

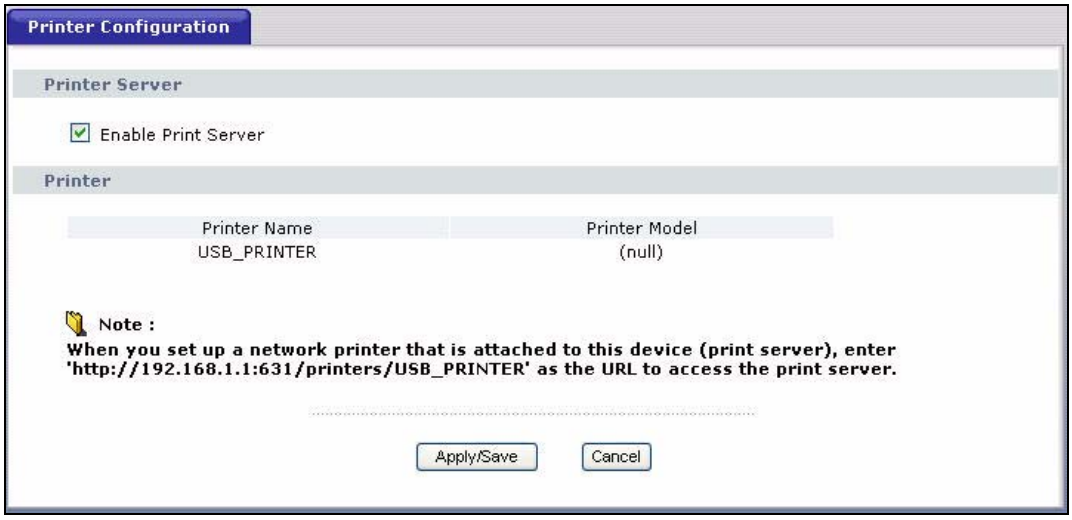
Note: Your printer's installation instructions may ask that you connect the printer to your computer. Connect your printer to the P-2812HNU-51c instead.

11.4 The Print Server Screen

The print server screen is used to enable the print server function on the P-2812HNU-51c and confirm that the P-2812HNU-51c and the USB printer are able to communicate successfully.

Click **USB Services > Print Server** to display the **Print Server** screen.

Figure 105 USB Services > Print Server



The following table describes the labels in this screen.

Table 71 USB Services > Print Server

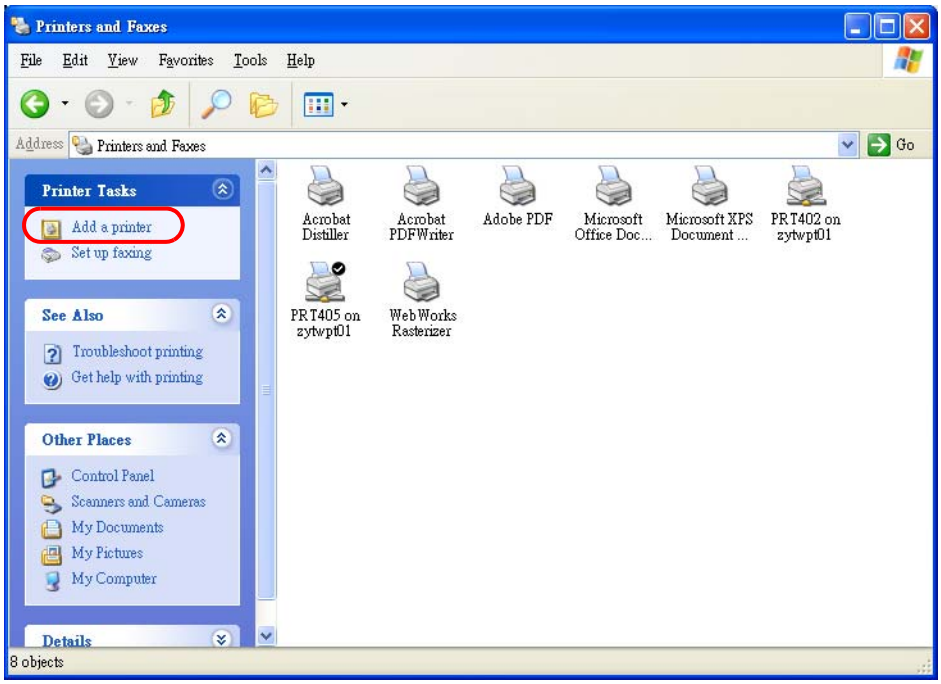
LABEL	DESCRIPTION
Enable Print Server	Select this option to have the P-2812HNU-51c act as a print server.
Printer Name	This displays the descriptive name of the associated printer for its recognition on the print server network. This name is displayed on a computer on the print server network when a print job is executed.
Printer Model	This displays the model name of the printer currently connected to the P-2812HNU-51c print server.
Apply/Save	Click **Apply/Save** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to return to the previous configuration.

11.5 Add a New Printer Using Windows

This example shows how to connect a printer behind the P-2812HNU-51c to your computer using the Windows XP Professional operating system. Some menu items may look different on your operating system.

1 Click **Start** > **Control Panel** > **Printers and Faxes** to open the **Printers and Faxes** screen. Click **Add a Printer**.

Figure 106 Printers Folder



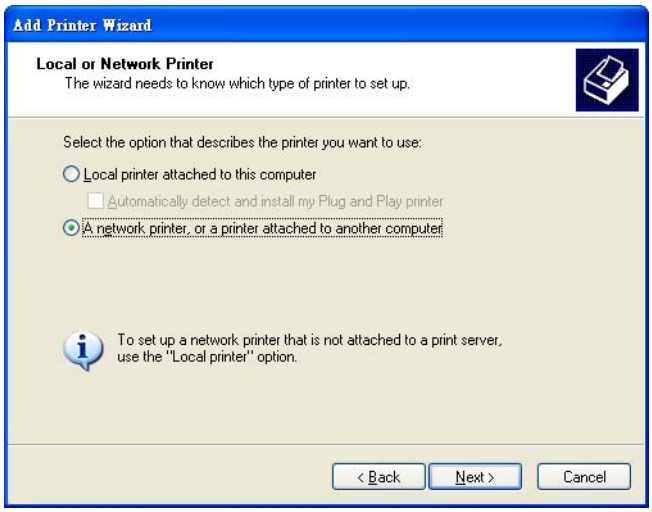
2 The **Add Printer Wizard** screen displays. Click **Next**.

Figure 107 Add Printer Wizard: Welcome

Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.
To continue, click Next.
< Back
Next >
Cancel

3 Select **A network printer, or a printer attached to another computer** and click **Next**.

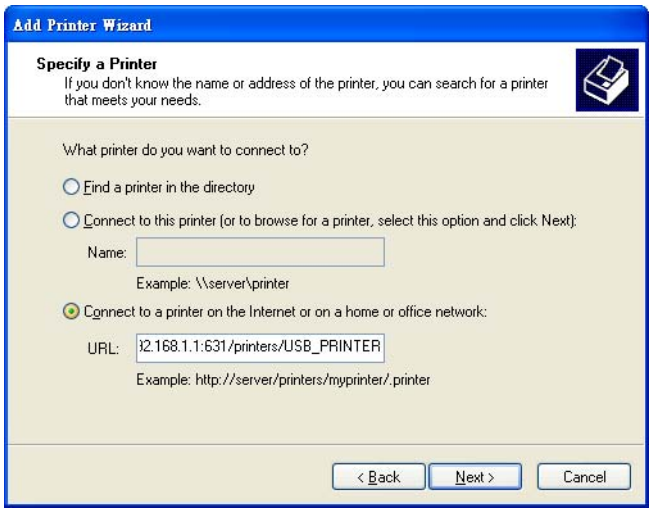
Figure 108 Add Printer Wizard: Local or Network Printer


Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< Back
Next >
Cancel

4 Select **Connect to a printer on the Internet or on a home or office network:** and enter “http://192.168.1.1:631/printers/USB_PRINTER” as the URL to access the print server (P-2812HNU-51c). Click **Next**.

Note: If you change the P-2812HNU-51c’s LAN IP address, use the new IP address in the URL to access the print server.

Figure 109 Add Printer Wizard: Specify a Printer


Add Printer Wizard
Specify a Printer
If you don't know the name or address of the printer, you can search for a printer that meets your needs.
What printer do you want to connect to?
Find a printer in the directory
Connect to this printer (or to browse for a printer, select this option and click Next):
Name:
Example: \\server\printer
Connect to a printer on the Internet or on a home or office network:
URL:
http://192.168.1.1:631/printers/USB_PRINTER
Example: http://server/printers/myprinter/.printer
< Back
Next >
Cancel

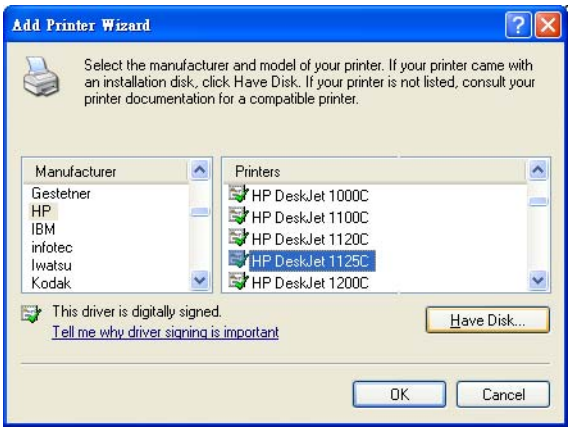
5 Select the make of the printer that you want to connect to the print server in the **Manufacturer** list of printers.

6 Select the printer model from the list of **Printers**.

7 If your printer is not displayed in the list of **Printers**, you can insert the printer driver installation CD/disk or download the driver file to your computer, click **Have Disk...** and install the new printer driver.

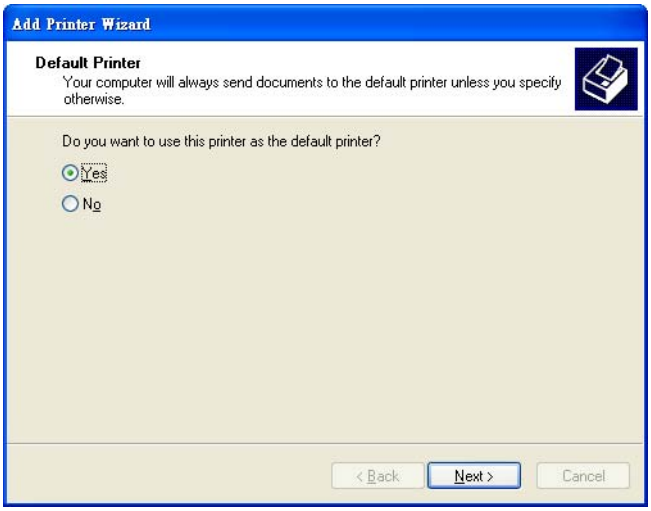
8 Click **Next** to continue.

Figure 110 Add Printer Wizard: Printer Model



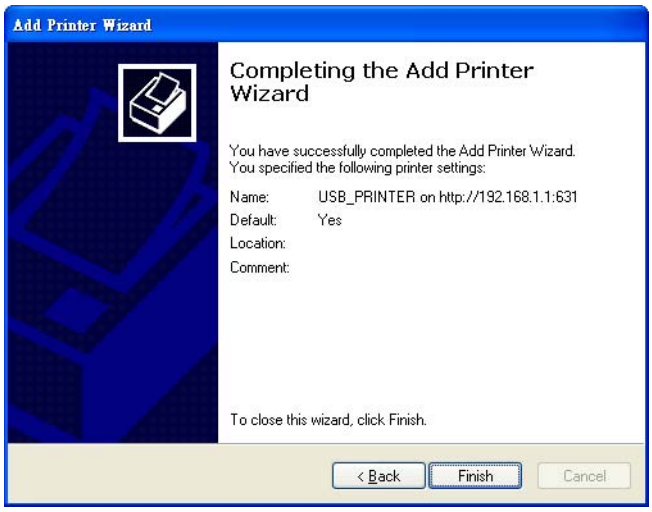
9 Select **Yes** and then click the **Next** button if you want to use this printer as the default printer on your computer. Otherwise select **No** and then click **Next** to continue.

Figure 111 Add Printer Wizard: Default Printer


Add Printer Wizard
Default Printer
Your computer will always send documents to the default printer unless you specify otherwise.
Do you want to use this printer as the default printer?
Yes
No
< Back
Next >
Cancel

10 The following screen shows your current printer settings. Select **Finish** to complete adding a new printer.

Figure 112 Add Printer Wizard Complete



11.6 Add a New Printer Using Macintosh OS X

Complete the following steps to set up a print server driver on your Macintosh computer.

11.6.1 Mac OS 10.3 and 10.4

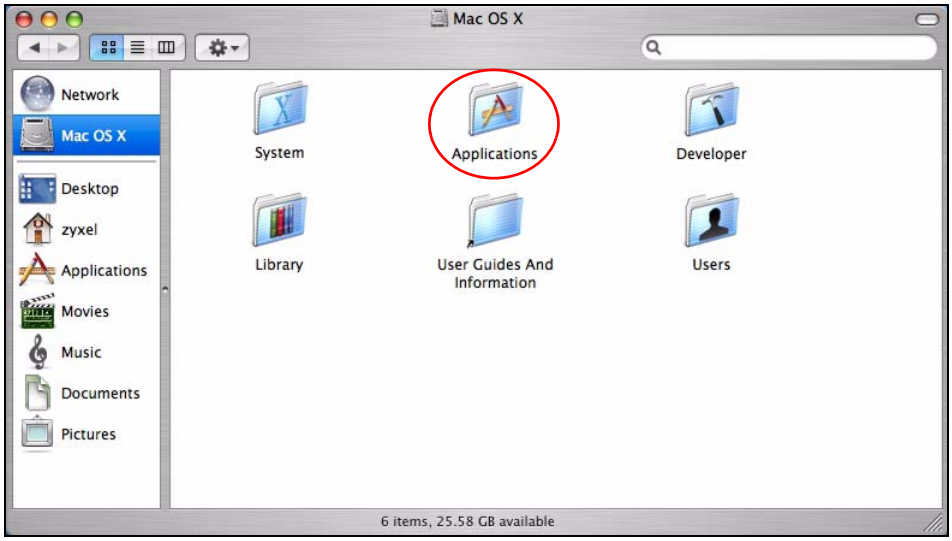
This example shows how to connect a printer behind the P-2812HNU-51c to your computer using Mac OS X v10.4.11. Some menu items may look different on your operating system.

11 Click the Finder icon on the Dock (a place holding a series of icons/shortcuts at the bottom of the desktop) or double-click your Mac hard disk icon (**Mac OS X** in this example) on your desktop to open the Mac HD window.

Figure 113 Mac OS X HD

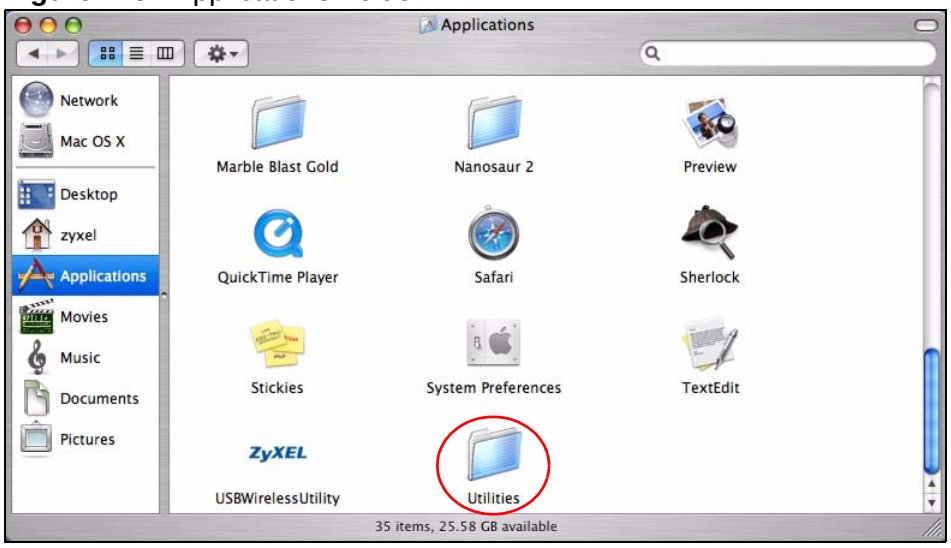
12 Open the **Applications** folder.

Figure 114 Macintosh HD Folder



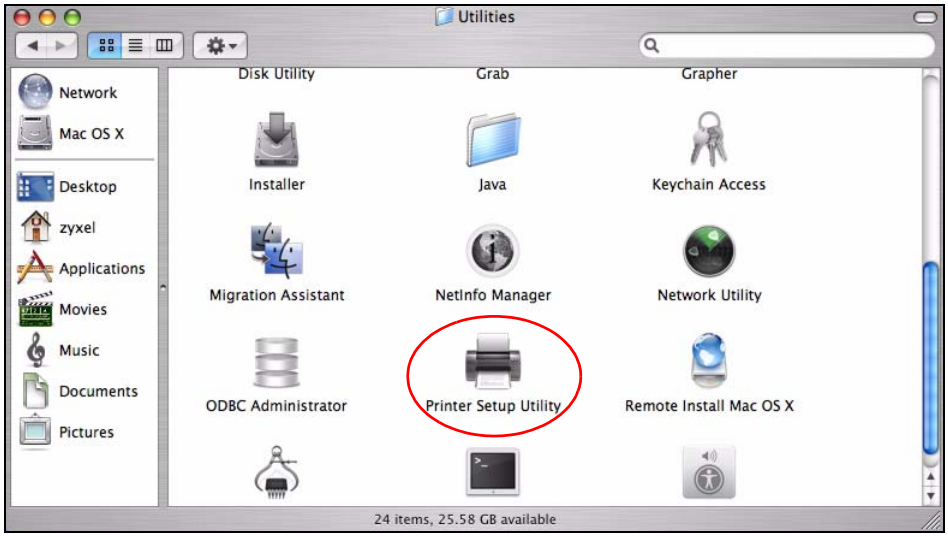
13 Open the **Utilities** folder.

Figure 115 Applications Folder



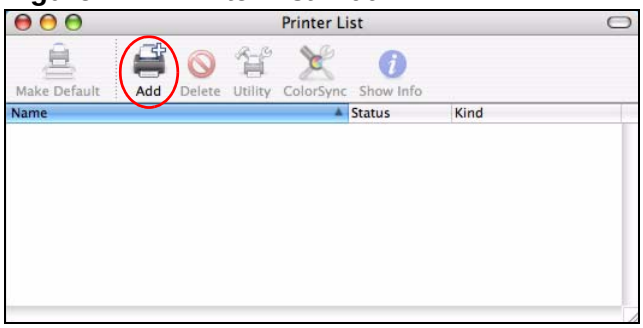
14 Double-click the **Printer Setup Utility** icon.

Figure 116 Utilities Folder



15 Click the **Add** icon at the top of the screen.

Figure 117 Printer List: Add



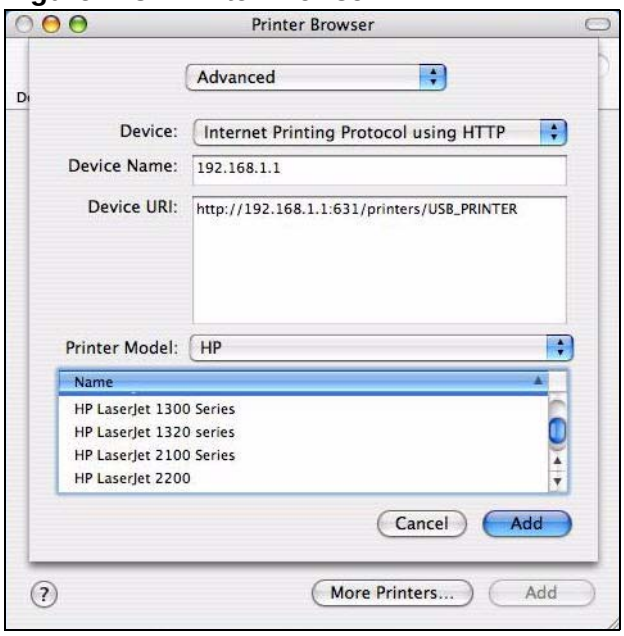
16 Click the **IP Printer** tab to set up your printer.

- Press the `alt` key and click **More Printers** in the **Printer Browser** screen.
- Select **Advanced** from the top drop-down list.
- Select **Internet Printing Protocol using HTTP** from the **Device** drop-down list.
- Enter a descriptive name for the printer in the **Device Name** field.
- In the **Device URL** field, enter “http://192.168.1.1:631/printers/USB_PRINTER” as the URL to access the print server (P-2812HNU-51c).

Note: If you change the P-2812HNU-51c’s LAN IP address, use the new IP address in the URL to access the print server.

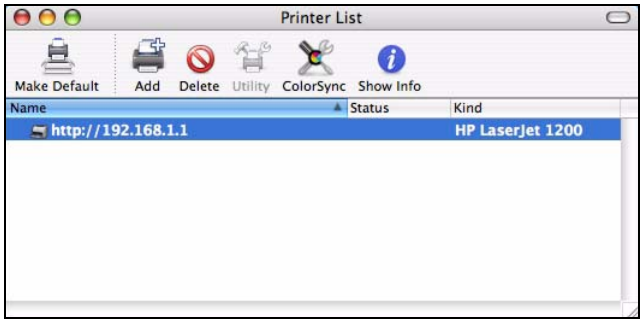
- Select your printer manufacturer from the **Printer Model** drop-down list and then select a printer model. Click **Add** to save and close the **Printer Browser** configuration screen.

Figure 118 Printer Browser



17 The new network printer displays in the **Printer List**. The default printer **Name** displays in bold type.

Figure 119 Printer List



18 Your print server driver setup is complete. You can now use the P-2812HNU-51c's print server to print from a Mac computer.

11.6.2 Mac OS 10.5 and 10.6

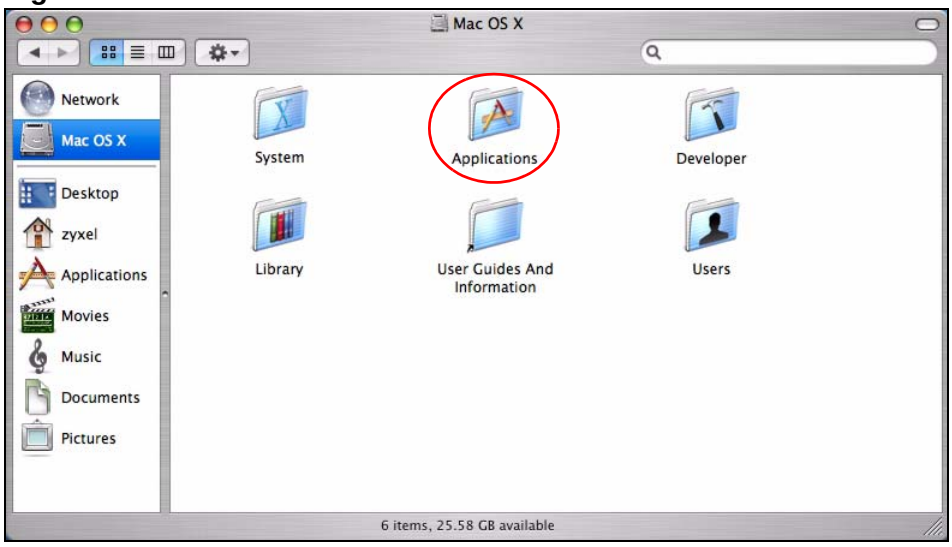
This example shows how to connect a printer behind the P-2812HNU-51c to your computer using Mac OS X v10.6.2. Some menu items may look different on your operating system.

1 Click the Finder icon on the Dock or double-click your Mac hard disk icon (**Mac OS X** in this example) on your desktop to open the Mac HD window.

Figure 120 Mac OS X HD

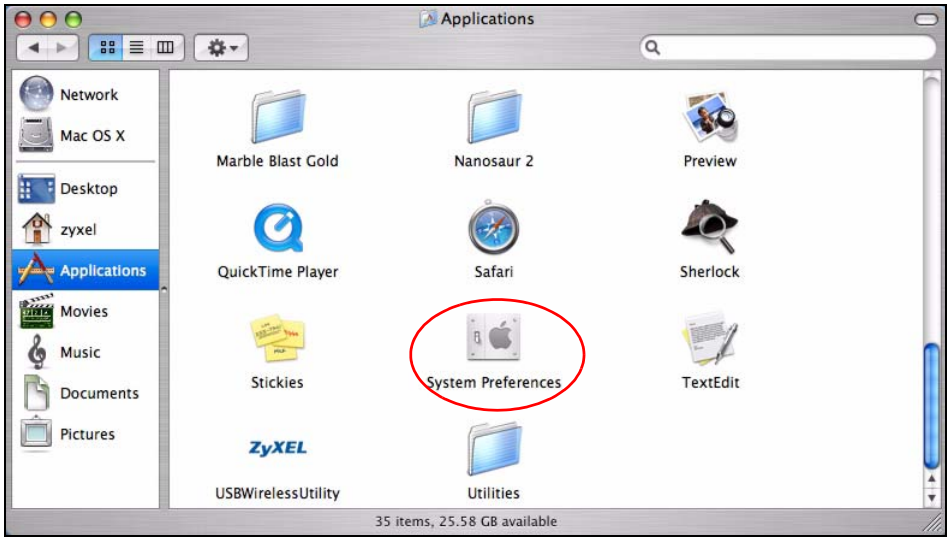
2 Open the **Applications** folder.

Figure 121 Macintosh HD Folder



3 Double-click the **System Preferences** icon.

Figure 122 Applications Folder

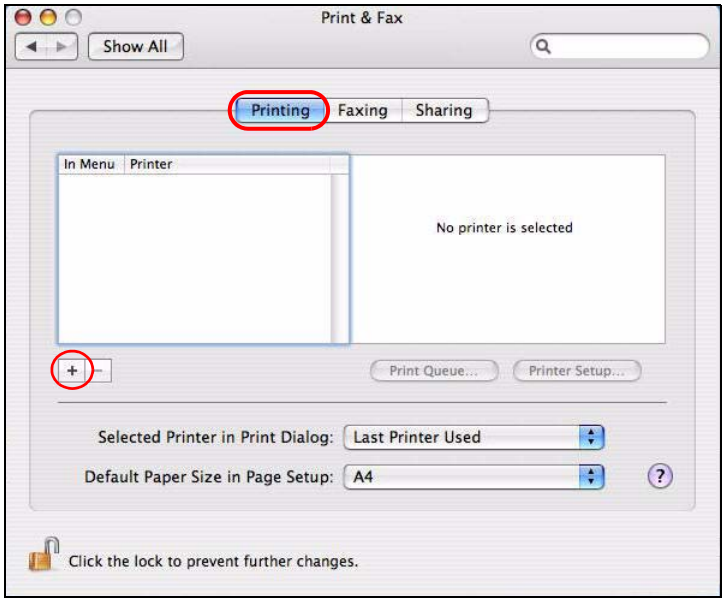


4 Click the **Print & Fax** icon.

Figure 123 System Preferences

5 Select the **Printing** tab and click the **+** icon to add a new printer.

Figure 124 Print & Fax



6 Click the **Advanced** button on the **Add Printer** toolbar to set up your printer.

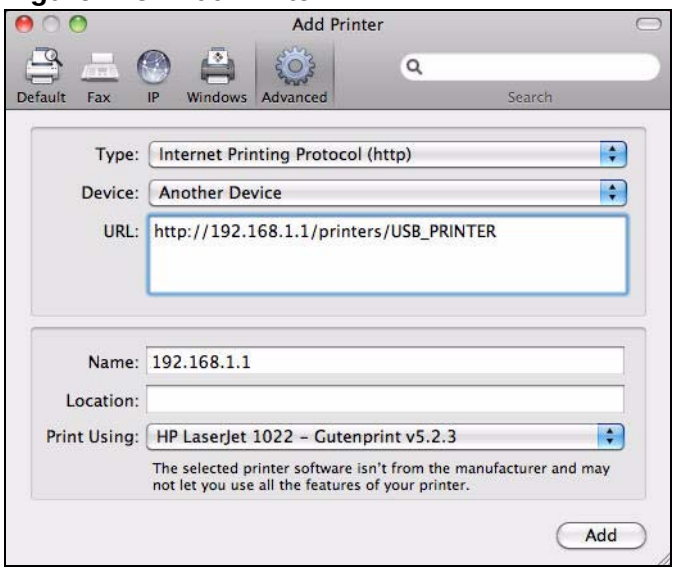
If the **Advanced** button doesn't appear, Ctrl-click the toolbar, select **Customize Toolbar...** and then drag the **Advanced** button onto the toolbar.

- Select **Internet Printing Protocol (HTTP)** from the **Type** drop-down list.
- Select **Another Device** from the **Device** drop-down list.
- In the **URL** field, enter "http://192.168.1.1:631/printers/USB_PRINTER" as the URL to access the print server (P-2812HNU-51c).

Note: If you change the P-2812HNU-51c's LAN IP address, use the new IP address in the URL to access the print server.

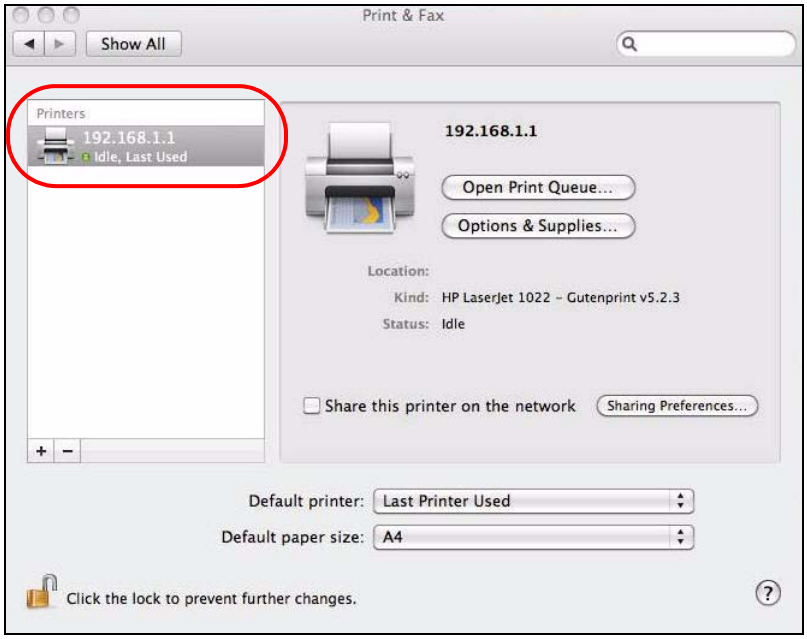
- Enter a descriptive name for the printer and where it is located.
- Select your printer manufacturer from the **Print Using** drop-down list and then select a printer model. Click **Add** to save and close the **Printer Browser** configuration screen.

Figure 125 Add Printer



7 The new network printer displays in the **Printers** list.

Figure 126 Printer List



8 Your print server driver setup is complete. You can now use the P-2812HNU-51c's print server to print from a Mac computer.

11.7 P-2812HNU-51c Print Server Compatible USB Printers

The following is a list of USB printer models compatible with the P-2812HNU-51c print server.

Table 72 Compatible USB Printers

BRAND	MODEL
CANON	MP-530
HP	DeskJet F380
HP	LaserJet 1022
LEXMARK	Z645
SAMSUNG	CLP-300

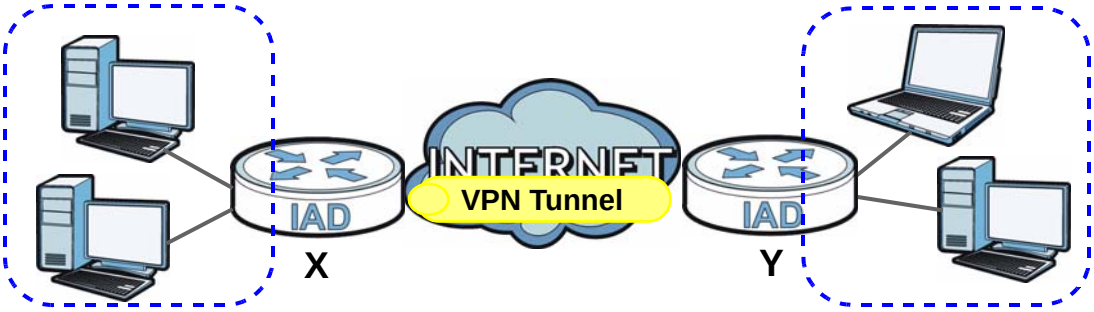
12 IPSec VPN

12.1 Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The following figure is an example of an IPSec VPN tunnel.

Figure 127 VPN: Example



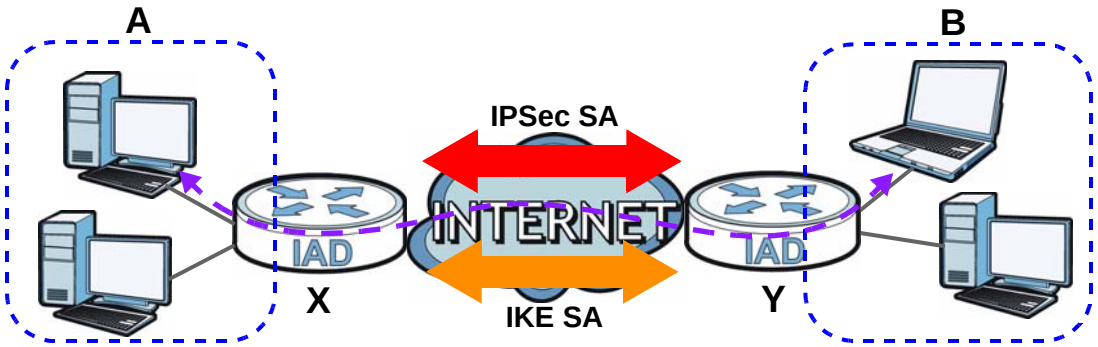
12.1.1 What You Can Do in this Chapter

- The **IPSec VPN** screen lets you view the configured VPN policies and add, edit or remove a VPN policy (Section 12.3 on page 255).
- The **Status** screen lets you display and manage the current active VPN connections (Section 12.4 on page 266).

12.2 What You Need to Know

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the P-2812HNU-51c and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the P-2812HNU-51c and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the P-2812HNU-51c and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 128 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

Remote IPSec Gateway Address

Remote IPSec Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Remote IPSec Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Remote IPSec Gateway Address** field.

You can also enter a remote IPSec gateway's domain name in the **Remote IPSec Gateway Address** field if the remote gateway has a dynamic WAN IP address and is using DDNS. The P-2812HNU-51c has to rebuild the VPN tunnel each time the remote gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

Finding Out More

See Section 12.5 on page 267 for advanced technical information on IPSec VPN.

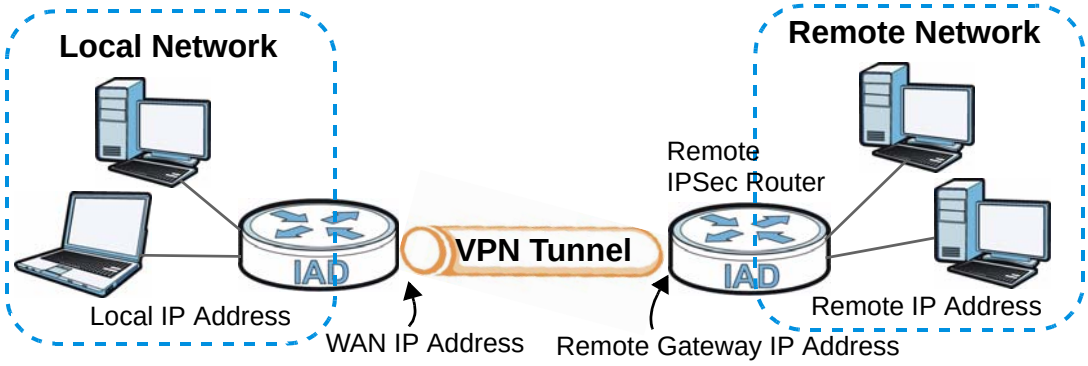
12.2.1 Before You Begin

If a VPN tunnel uses Telnet, FTP, WWW, then you should configure remote management (**Remote MGMT**) to allow access for that service.

12.3 The IPSec Screen

The following figure helps explain the main fields in the web configurator.

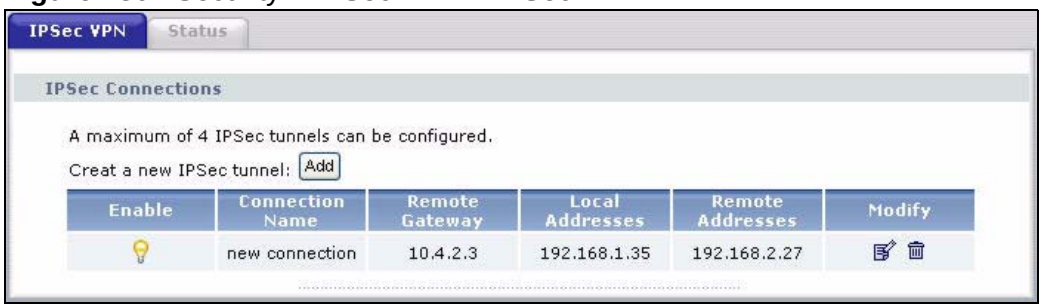
Figure 129 IPSec Summary Fields



Local and remote IP addresses must be static.

Click **Security** > **IPSec VPN** to open the **IPSec VPN** screen. This is a menu of your IPSec rules (tunnels). The IPSec summary menu is read-only. Edit a VPN by clicking the **Add** button or a rule's **Edit** icon and then configuring its associated submenus.

Figure 130 Security > IPSec VPN > IPSec VPN



The following table describes the fields in this screen.

Table 73 Security > IPSec VPN > IPSec VPN

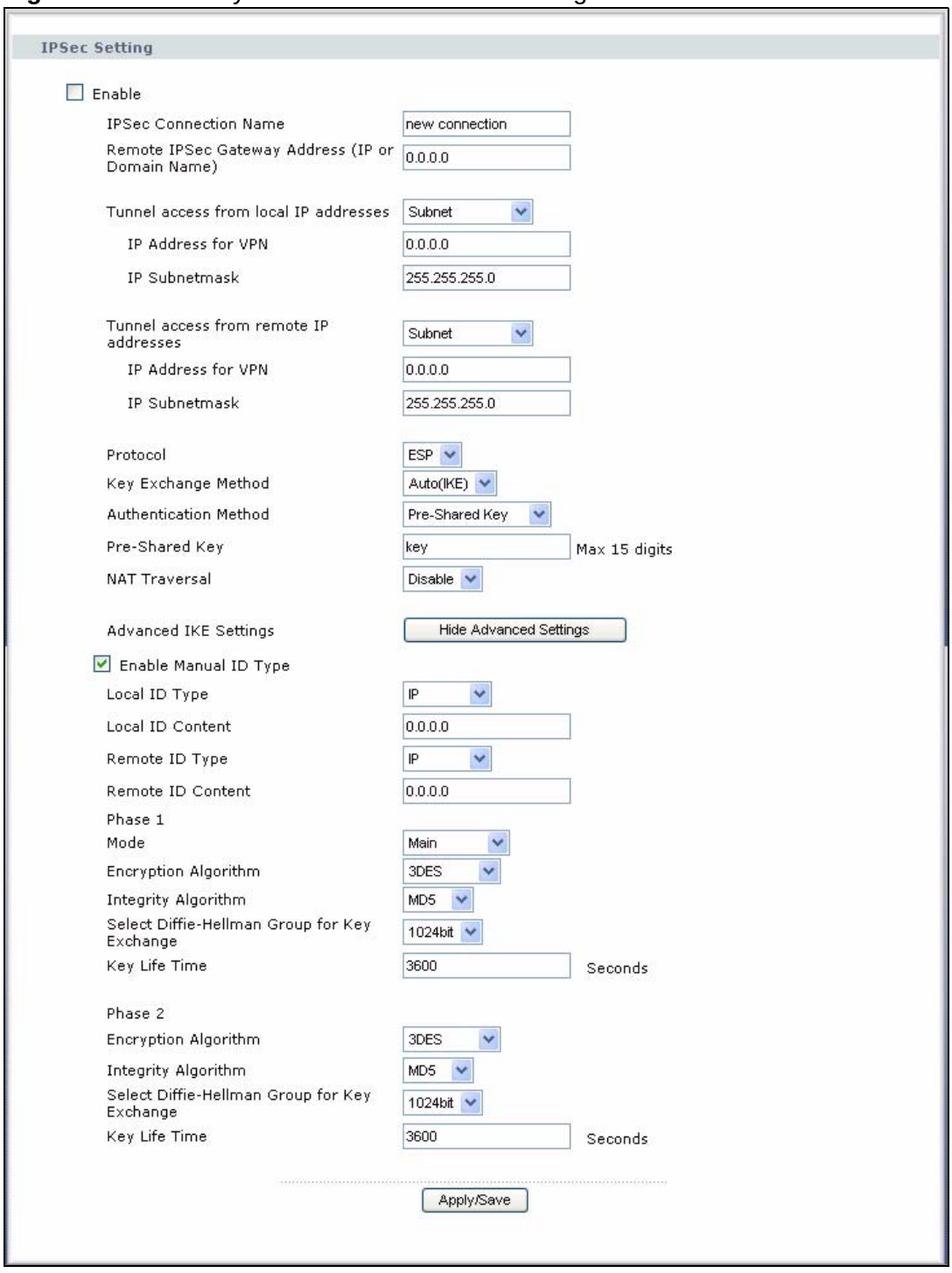
LABEL	DESCRIPTION
Add	Click this button to configure a new VPN policy.
Enable	This field displays whether the VPN policy is active or not. A yellow bulb signifies that this VPN policy is active. A gray bulb signifies that this VPN policy is not active.
Connection Name	This field displays the identification name for this VPN policy.
Remote Gateway	This is the static WAN IP address or URL of the remote IPSec router.
Local Addresses	This is the IP address of computer(s) on your local network behind your P-2812HNU-51c.
Remote Addresses	This is the IP address of computer(s) on the remote network behind the remote IPSec router.
Modify	Click the **Edit** icon to go to the screen where you can edit the VPN configuration. Click the **Remove** icon to remove an existing VPN configuration.

12.3.1 The IPSec Setting Screen

Click the **Add** button or a policy's **Edit** icon in the **IPSec VPN** screen to edit VPN policies.

Note: The P-2812HNU-51c uses the system default gateway interface's WAN IP address as its WAN IP address to set up a VPN tunnel.

Figure 131 Security > IPSec VPN > IPSec Setting > IKE



The following table describes the fields in this screen.

Table 74 Security > IPSec VPN > IPSec Setting > IKE

LABEL	DESCRIPTION
IPSec Setting	
Enable	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
IPSec Connection Name	Type up to 60 alphanumeric characters to identify this VPN policy. You may use spaces, underscores and dashes, but the P-2812HNU-51c drops trailing spaces.
Remote IPSec Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Tunnel access from local IP addresses	Specify the IP addresses of the devices behind the P-2812HNU-51c that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Use the drop-down menu to choose **Single Address** or **Subnet**. Select **Single Address** for a single IP address. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address for VPN	When the local IP address type is configured to **Single Address**, enter a (static) IP address on the LAN behind your P-2812HNU-51c. When the local IP address type is configured to **Subnet**, enter a (static) IP address on the LAN behind your P-2812HNU-51c.
IP Subnetmask	When the local IP address type is configured to **Single Address**, this field is not available. When the local IP address type is configured to **Subnet**, enter a subnet mask on the LAN behind your P-2812HNU-51c.
Tunnel access from remote IP addresses	Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Use the drop-down menu to choose **Single Address** or **Subnet**. Select **Single Address** with a single IP address. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address for VPN	When the remote IP address type is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the remote IP address type is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.

Table 74 Security > IPSec VPN > IPSec Setting > IKE (continued)

LABEL	DESCRIPTION
IP Subnetmask	When the remote IP address type is configured to **Single Address**, this field is not available. When the remote IP address type is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Protocol	This field displays **ESP** and the P-2812HNU-51c uses ESP (Encapsulation Security Payload) for VPN. The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**.
Key Exchange Method	Select **Auto(IKE)** or **Manual** from the drop-down list box. **Auto(IKE)** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **Auto(IKE)** key management.
Authentication Method	Select **Pre-Shared Key** to use a pre-shared key for authentication. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Select **Certificates (X.509)** to use a certificate for authentication.
Pre-Shared Key	This field is available only when you select **Pre-Shared Key** in the **Authentication Method** field. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Certificates	This field is available only when you select **Certificates** in the **Authentication Method** field. Select the certificate you want to use from the drop-down list box. You can create, import and configure certificates in the **Security > Certificates** screens.
NAT Traversal	Select **Enable** if you want to set up a VPN tunnel when there are NAT routers between the P-2812HNU-51c and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 500 packets to the remote IPSec router behind the NAT router. Otherwise, select **Disable**.
Advanced IKE Settings	Click **Show Advanced Settings** to display and configure more detailed settings of your IKE key management. Otherwise, click **Hide Advanced Settings**.
Enable Manual ID Type	Select this option to specify how to identify the P-2812HNU-51c and remote IPSec router.

Table 74 Security > IPSec VPN > IPSec Setting > IKE (continued)

LABEL	DESCRIPTION
Local ID Type	Select **IP** to identify this P-2812HNU-51c by its IP address. Select **DNS** to identify this P-2812HNU-51c by a domain name. Select **E-mail** to identify this P-2812HNU-51c by an e-mail address. Select **ASN1DN** (Abstract Syntax Notation one - Distinguished Name) to identify the remote IPSec router by the subject field in a certificate. This is used only with certificate-based authentication.
Local ID Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the **Local ID Content** field. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this P-2812HNU-51c in the **Local ID Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address. Select **ASN1DN** (Abstract Syntax Notation one - Distinguished Name) to identify the remote IPSec router by the subject field in a certificate. This is used only with certificate-based authentication.
Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Phase 1/Phase 2	
Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	Select **DES**, **3DES**, **AES-128**, **ES-192** or **AES-256** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit, 192-bit or 256-bit key. **AES** is faster than **3DES**.

Table 74 Security > IPSec VPN > IPSec Setting > IKE (continued)

LABEL	DESCRIPTION
Integrity Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Select Diffie-Hellman Group for Key Exchange	You must choose a key group for key exchange in SA setup. **768bit** refers to Diffie-Hellman Group 1 a 768 bit random number. **1024bit** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. Other options include 1536, 2048, and 3072 bit Diffie-Hellman groups.
Key Life Time (Seconds)	Define the length of time before an IKE or IPSec SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Apply/Save	Click **Apply/Save** to save your changes back to the P-2812HNU-51c and return to the **IPSec** screen.

12.3.2 Manual Key Setup

Manual key management is useful if you have problems with **Auto(IKE)** key management.

12.3.2.1 Security Parameter Index (SPI)

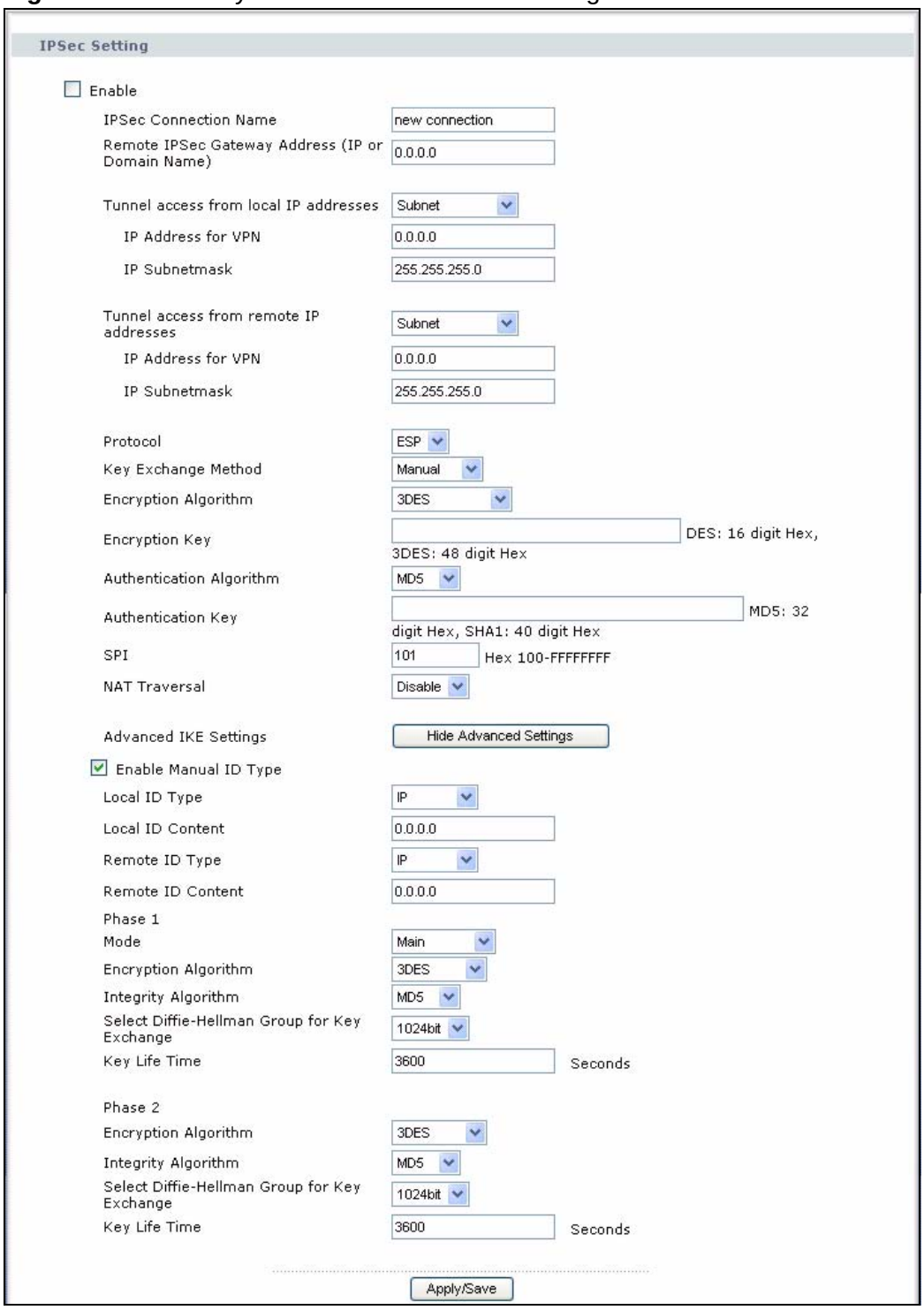
An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

12.3.3 Configuring Manual Key

You only configure VPN manual key when you select **Manual** in the **Key Exchange Method** field on the **IPSec Setting** screen. This is the **IPSec Setting - Manual** screen as shown next.

Figure 132 Security > IPSec VPN > IPSec Setting > Manual



The following table describes the fields in this screen.

Table 75 Security > IPSec VPN > IPSec Setting > Manual

LABEL	DESCRIPTION
IPSec Setting	
Enable	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
IPSec Connection Name	Type up to 60 alphanumeric characters to identify this VPN policy. You may use spaces, underscores and dashes, but the P-2812HNU-51c drops trailing spaces.
Remote IPSec Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Tunnel access from local IP addresses	Specify the IP addresses of the devices behind the P-2812HNU-51c that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Use the drop-down menu to choose **Single Address** or **Subnet**. Select **Single Address** for a single IP address. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address for VPN	When the local IP address type is configured to **Single Address**, enter a (static) IP address on the LAN behind your P-2812HNU-51c. When the local IP address type is configured to **Subnet**, enter a (static) IP address on the LAN behind your P-2812HNU-51c.
IP Subnetmask	When the local IP address type is configured to **Single Address**, this field is not available. When the local IP address type is configured to **Subnet**, enter a subnet mask on the LAN behind your P-2812HNU-51c.
Tunnel access from remote IP addresses	Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Use the drop-down menu to choose **Single Address** or **Subnet**. Select **Single Address** with a single IP address. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address for VPN	When the remote IP address type is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the remote IP address type is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.

Table 75 Security > IPSec VPN > IPSec Setting > Manual (continued)

LABEL	DESCRIPTION
IP Subnetmask	When the remote IP address type is configured to **Single Address**, this field is not available. When the remote IP address type is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Protocol	This field displays **ESP** and the P-2812HNU-51c uses ESP (Encapsulation Security Payload) for VPN. The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**.
Key Exchange Method	Select **Auto(IKE)** or **Manual** from the drop-down list box. **Auto(IKE)** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **Auto(IKE)** key management.
Encryption Algorithm	Select **DES**, **3DES**, **AES(aes-cbc)** or **ESP_NULL** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES(aes-cbc)** in Cipher Block Chaining (CBC) mode uses a 128-bit key. **AES** is faster than **3DES**. Select **ESP_NULL** to set up a tunnel without encryption. When you select **ESP_NULL**, you do not enter an encryption key.
Encryption Key	Type 16 hexadecimal ("0-9", "A-F") characters if you select to use the DES encryption algorithm or 48 hexadecimal characters if you use the 3DES encryption algorithm.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Authentication Key	Type 32 hexadecimal ("0-9", "A-F") characters if you select to use the MD5 authentication algorithm or 40 hexadecimal characters if you use the SHA1 authentication algorithm.
SPI	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.
NAT Traversal	Select **Enable** if you want to set up a VPN tunnel when there are NAT routers between the P-2812HNU-51c and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 500 packets to the remote IPSec router behind the NAT router. Otherwise, select **Disable**.
Advanced IKE Settings	Click **Show Advanced Settings** to display and configure more detailed settings of your IKE key management. Otherwise, click **Hide Advanced Settings**.
Enable Manual ID Type	Select this option to specify how to identify the P-2812HNU-51c and remote IPSec router.

Table 75 Security > IPSec VPN > IPSec Setting > Manual (continued)

LABEL	DESCRIPTION
Local ID Type	Select **IP** to identify this P-2812HNU-51c by its IP address. Select **DNS** to identify this P-2812HNU-51c by a domain name. Select **E-mail** to identify this P-2812HNU-51c by an e-mail address. Select **ASN1DN** (Abstract Syntax Notation one - Distinguished Name) to identify the remote IPSec router by the subject field in a certificate. This is used only with certificate-based authentication.
Local ID Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the **Local ID Content** field. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this P-2812HNU-51c in the **Local ID Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address. Select **ASN1DN** (Abstract Syntax Notation one - Distinguished Name) to identify the remote IPSec router by the subject field in a certificate. This is used only with certificate-based authentication.
Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Phase 1/Phase 2	
Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	Select **DES**, **3DES**, **AES-128**, **ES-192** or **AES-256** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit, 192-bit or 256-bit key. **AES** is faster than **3DES**.

Table 75 Security > IPSec VPN > IPSec Setting > Manual (continued)

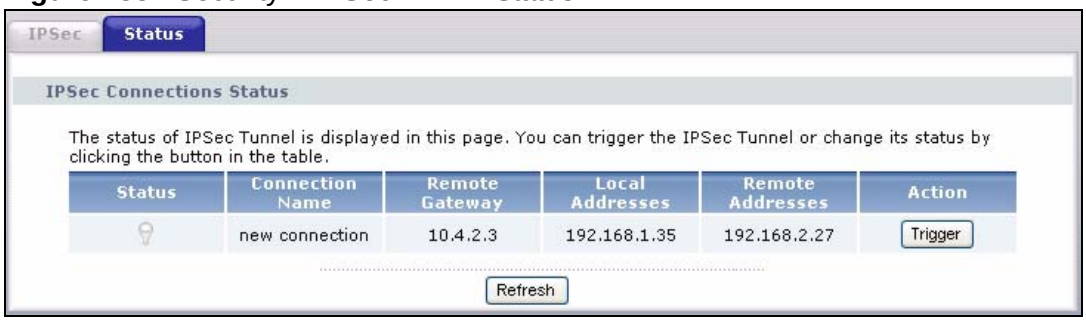
LABEL	DESCRIPTION
Integrity Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Select Diffie-Hellman Group for Key Exchange	You must choose a key group for key exchange in SA setup. **768bit** refers to Diffie-Hellman Group 1 a 768 bit random number. **1024bit** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. Other options include 1536, 2048, and 3072 bit Diffie-Hellman groups.
Key Life Time (Seconds)	Define the length of time before an IKE or IPSec SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Apply/Save	Click **Apply/Save** to save your changes back to the P-2812HNU-51c and return to the **IPSec** screen.

12.4 Viewing VPN Status

Click **Security** > **IPSec VPN** > **Status** to open the screen as shown. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.

Figure 133 Security > IPSec VPN > Status



The following table describes the fields in this screen.

Table 76 Security > IPSec VPN > Status

LABEL	DESCRIPTION
Status	This field displays whether the VPN connection is up (a yellow bulb) or down (a gray bulb).
Connection Name	This field displays the identification name for this VPN policy.
Remote Gateway	This is the static WAN IP address or URL of the remote IPSec router.
Local Addresses	This is the IP address of computer(s) on your local network behind your P-2812HNU-51c.
Remote Addresses	This is the IP address of computer(s) on the remote network behind the remote IPSec router.
Action	Click **Trigger** to establish a VPN connection with the remote network.
Refresh	Click **Refresh** to display the current active VPN connection(s).

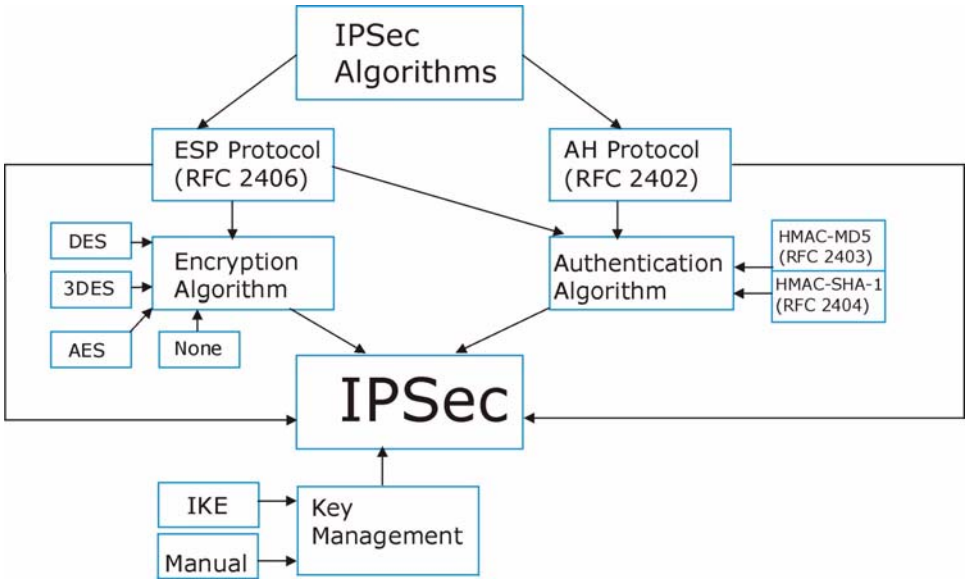
12.5 IPSec VPN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

12.5.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 134 IPSec Architecture



IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

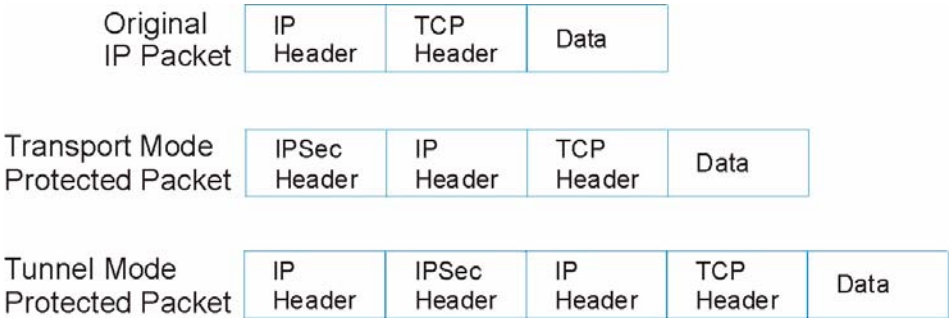
Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

12.5.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the P-2812HNU-51c supports **Tunnel** mode only.

Figure 135 Transport and Tunnel Mode IPSec Encapsulation



Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

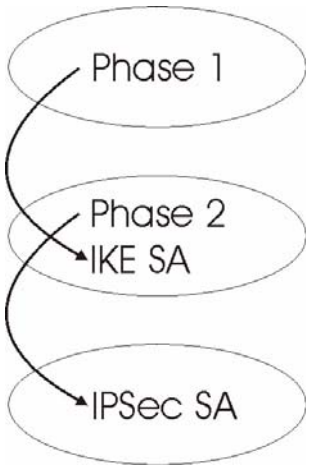
Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

12.5.3 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 136 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.

- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The P-2812HNU-51c automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

12.5.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

12.5.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the P-2812HNU-51c.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash

value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 77 VPN and NAT

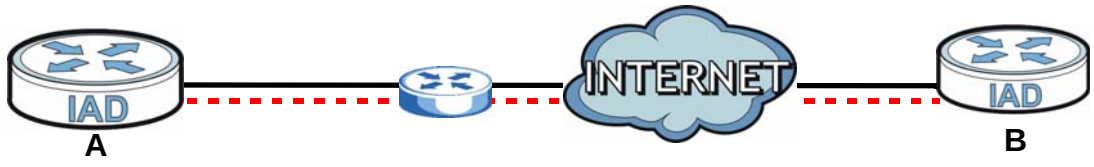
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

12.5.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the P-2812HNU-51c's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 137 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In Figure 137 on page 271, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 78 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the P-2812HNU-51c if you enable NAT traversal.

12.5.7 ID Type and Content

With aggressive negotiation mode (see Section 12.5.4 on page 270), the P-2812HNU-51c identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the P-2812HNU-51c to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the P-2812HNU-51c does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 12.5.4 on page 270), the ID type and content are encrypted to provide identity protection. In this case the P-2812HNU-51c can only distinguish between up to 12 different incoming SAs that connect from remote

IPSec routers that have dynamic WAN IP addresses. The P-2812HNU-51c can distinguish up to 48 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see Section 12.3 on page 255). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 79 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer.
DNS	Type a domain name (up to 31 characters) by which to identify this P-2812HNU-51c.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this P-2812HNU-51c.
	The domain name or e-mail address that you use in the **Local ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

Table 80 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
	The domain name or e-mail address that you use in the **Remote ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Remote IPSec Gateway Address** field below.

12.5.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two P-2812HNU-51cs in this example can complete negotiation and establish a VPN tunnel.

Table 81 Matching ID Type and Content Configuration Example

P-2812HNU-51C A	P-2812HNU-51C B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Remote ID type: IP	Remote ID type: E-mail
Remote ID content: 1.1.1.2	Remote ID content: tom@yourcompany.com

The two P-2812HNU-51cs in this example cannot complete their negotiation because P-2812HNU-51c B's **Local ID type** is **IP**, but P-2812HNU-51c A's **Remote ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 82 Mismatching ID Type and Content Configuration Example

P-2812HNU-51C A	P-2812HNU-51C B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.2
Remote ID type: E-mail	Remote ID type: IP
Remote ID content: aa@yahoo.com	Remote ID content: 1.1.1.0

12.5.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 12.5.3 on page 269 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

12.5.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit, 1024-bit 1536-bit, 2048-bit, and 3072-bit Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

13

Firewall

13.1 Overview

This chapter shows you how to enable and configure the P-2812HNU-51c firewall settings.

The P-2812HNU-51c firewall is a packet filtering firewall and restricts access based on the source/destination computer network address of a packet and the type of application.

13.1.1 What You Can Do in this Chapter

The **Incoming** screen lets you view and configure incoming IP filtering rules (Section 13.3 on page 276).

13.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An “extension number”, called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 83 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

Default Filtering Policies

Filtering rules are grouped based on the direction of travel of packets to which they apply.

The default rule for incoming traffic blocks all incoming connections from the WAN to the LAN. If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

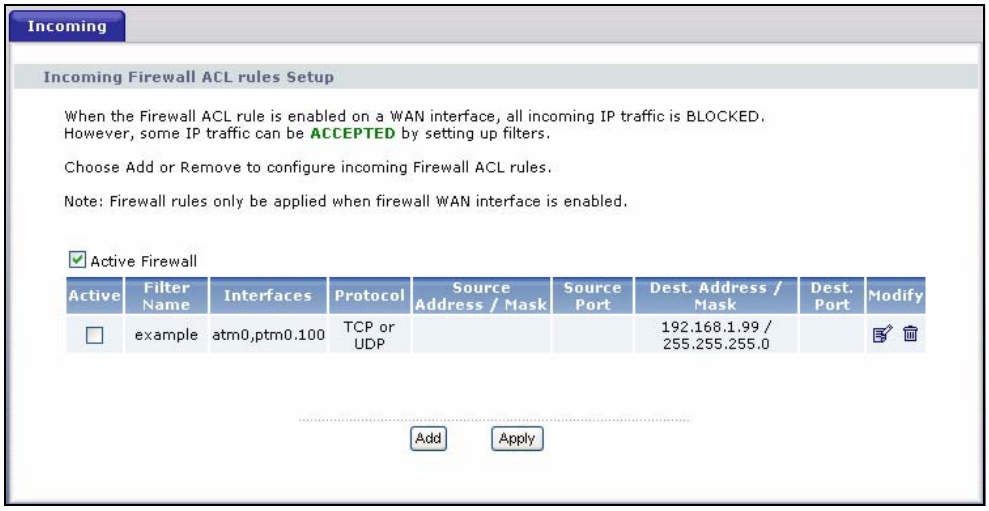
Note: If you configure filtering rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the P-2812HNU-51c's default rules.

13.3 The Firewall Screen

Click **Security > Firewall > Incoming** to display the following screen. This screen displays a list of the configured incoming filtering rules.

Figure 138 Firewall > Incoming



The following table describes the labels in this screen.

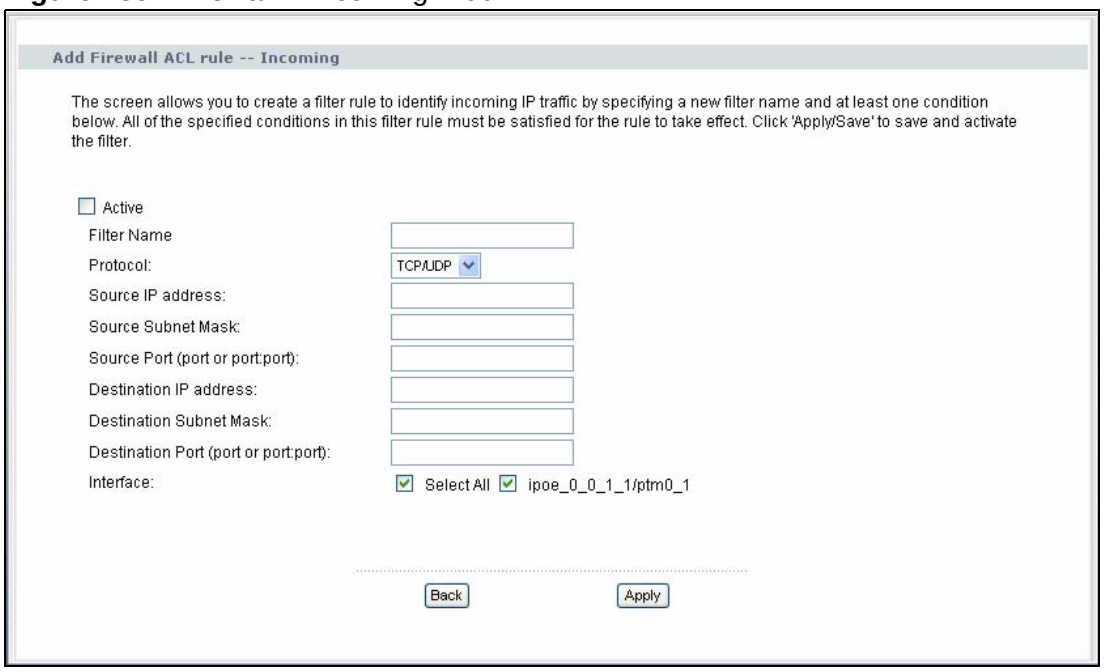
Table 84 Firewall > Incoming

LABEL	DESCRIPTION
Active Firewall	Select this check box to enable the firewall on the P-2812HNU-51c. When the firewall is enabled, the P-2812HNU-51c blocks all incoming traffic from the WAN to the LAN. Create custome rules below to allow certain WAN users to access your LAN or to allow traffic from the WAN to a certain computer on the LAN.
Active	Select this check box to enable the rule.
Filter Name	This displays the name of the rule.
Interfaces	This displays the WAN interface(s) to which this rule is applied.
Protocol	This displays the transport layer protocol that defines the service to which this rule applies.
Source Address / Mask	This displays the source IP addresses and subnet mask to which this rule applies. Please note that a blank source address is equivalent to **Any**.
Source Port	This is the source port number.
Dest. Address / Mask	This displays the destination IP addresses and subnet mask to which this rule applies. Please note that a blank destination address is equivalent to **Any**.
Dest. Port	This is the destination port number.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Remove** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.
Add	Click **Add** to create a new rule.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.

13.3.1 Creating Incoming Firewall Rules

In the **Incoming** screen, click **Add** to display this screen and refer to the following table for information on the labels.

Figure 139 Firewall > Incoming: Add


Add Firewall ACL rule -- Incoming
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.
Active
Filter Name
Protocol:
TCP/UDP
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):
Interface:
Select All
ipoe_0_0_1_1/ptm0_1
Back
Apply

The following table describes the labels in this screen.

Table 85 Firewall > Incoming: Add

LABEL	DESCRIPTION
Active	Select this check box to enable the rule.
Filter Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces. To add a firewall rule, you need to configure at least one of the following fields (except the **Interface** field).
Protocol	Select the transport layer protocol (**TCP/UDP**, **TCP**, **UDP** or **ICMP**) and enter the protocol (service type) number in the port field. Select **NONE** to apply the rule to any protocol.
Source IP Address	Enter the source IP address in dotted decimal notation.
Source Subnet Mask	Enter the source subnet mask.
Source Port	Enter a single port number or the range of port numbers of the source.
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter the port number of the destination.

Table 85 Firewall > Incoming: Add (continued)

LABEL	DESCRIPTION
Interface	Select **Select All** to apply the rule to all interfaces on the P-2812HNU-51c or select the specific WAN interface(s) to which this rule applies.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.

14

Certificate

14.1 Overview

The P-2812HNU-51c can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

14.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the P-2812HNU-51c's CA-signed certificates (Section 14.4 on page 289).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the P-2812HNU-51c (Section 14.4 on page 289).

14.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the P-2812HNU-51c to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

Certificate File Format

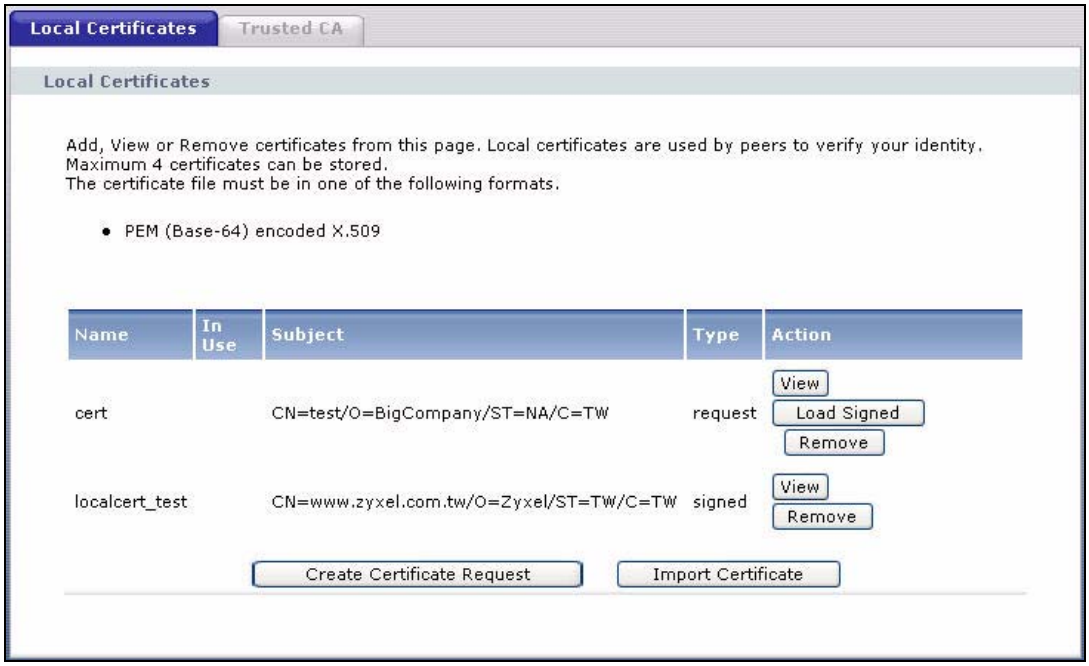
The certification authority certificate that you want to import has to be in one of these file formats:

- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

14.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the P-2812HNU-51c's summary list of certificates and certification requests.

Figure 140 Local Certificates



The following table describes the labels in this screen.

Table 86 Local Certificates

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
In Use	This field displays how many applications use the certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Type	This field displays what kind of certificate this is. **request** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **Load Certificate** screen to import the certificate and replace the request. **signed** represents a certificate issued by a certification authority.

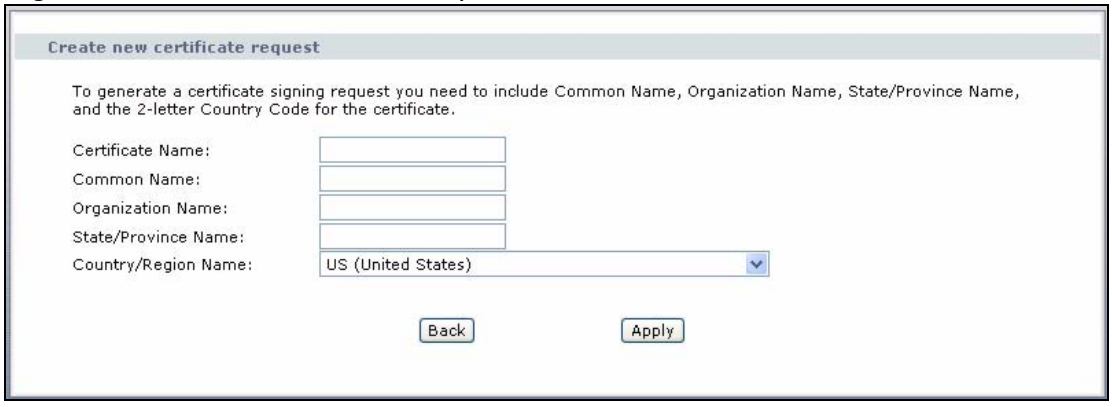
Table 86 Local Certificates (continued)

LABEL	DESCRIPTION
Modify	Click the **View** button to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Load Signed** button to import a valid certification to replace the request. Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.
Create Certificate Request	Click this button to go to the screen where you can have the P-2812HNU-51c generate a certification request.
Import Certificate	Click this button to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the P-2812HNU-51c.

14.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the **My Certificate Create** screen. Use this screen to have the P-2812HNU-51c generate a certification request.

Figure 141 Create Certificate Request


Create new certificate request
To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.
Certificate Name:
Common Name:
Organization Name:
State/Province Name:
Country/Region Name:
US (United States)
Back
Apply

The following table describes the labels in this screen.

Table 87 Create Certificate Request

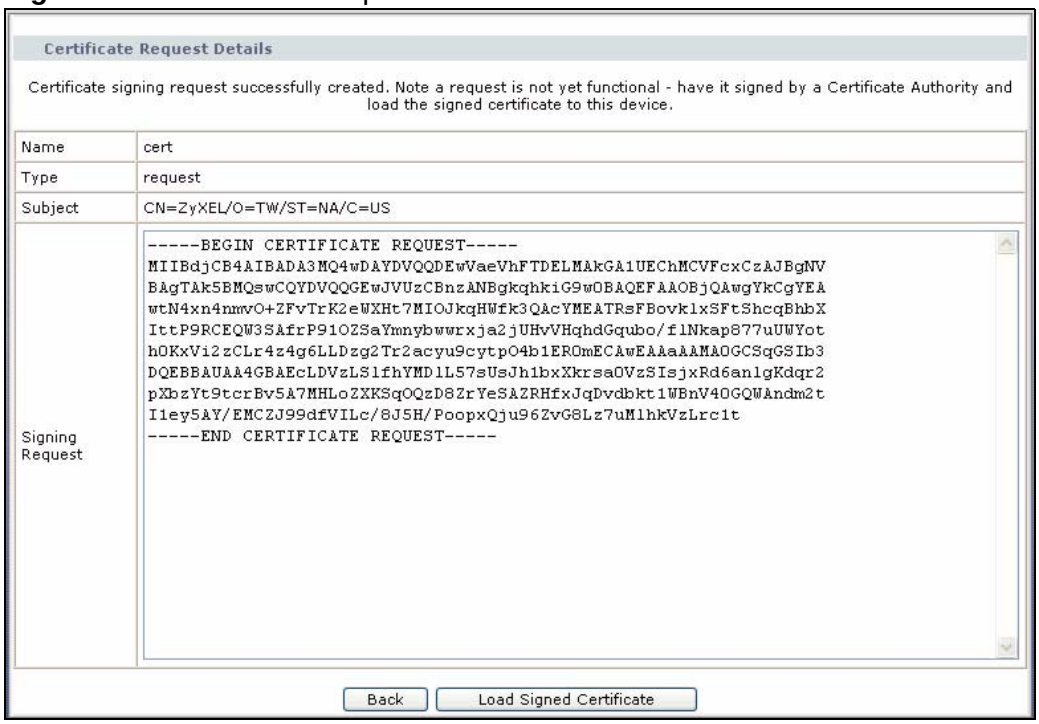
LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.

Table 87 Create Certificate Request (continued)

LABEL	DESCRIPTION
Organization Name	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the P-2812HNU-51c drops trailing spaces.
State/Province Name	Type up to 127 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the P-2812HNU-51c drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to begin certificate or certification request generation.

After you click **Apply**, the **Certificate Request Details** screen displays. Click **Load Signed Certificate** to import a certificate signed by the CA to replace the request (see Section 14.3.4 on page 288). Otherwise, click **Back** to return to the **Local Certificates** screen. See Section 14.3.3 on page 286 for field information.

Figure 142 Certificate Request Details

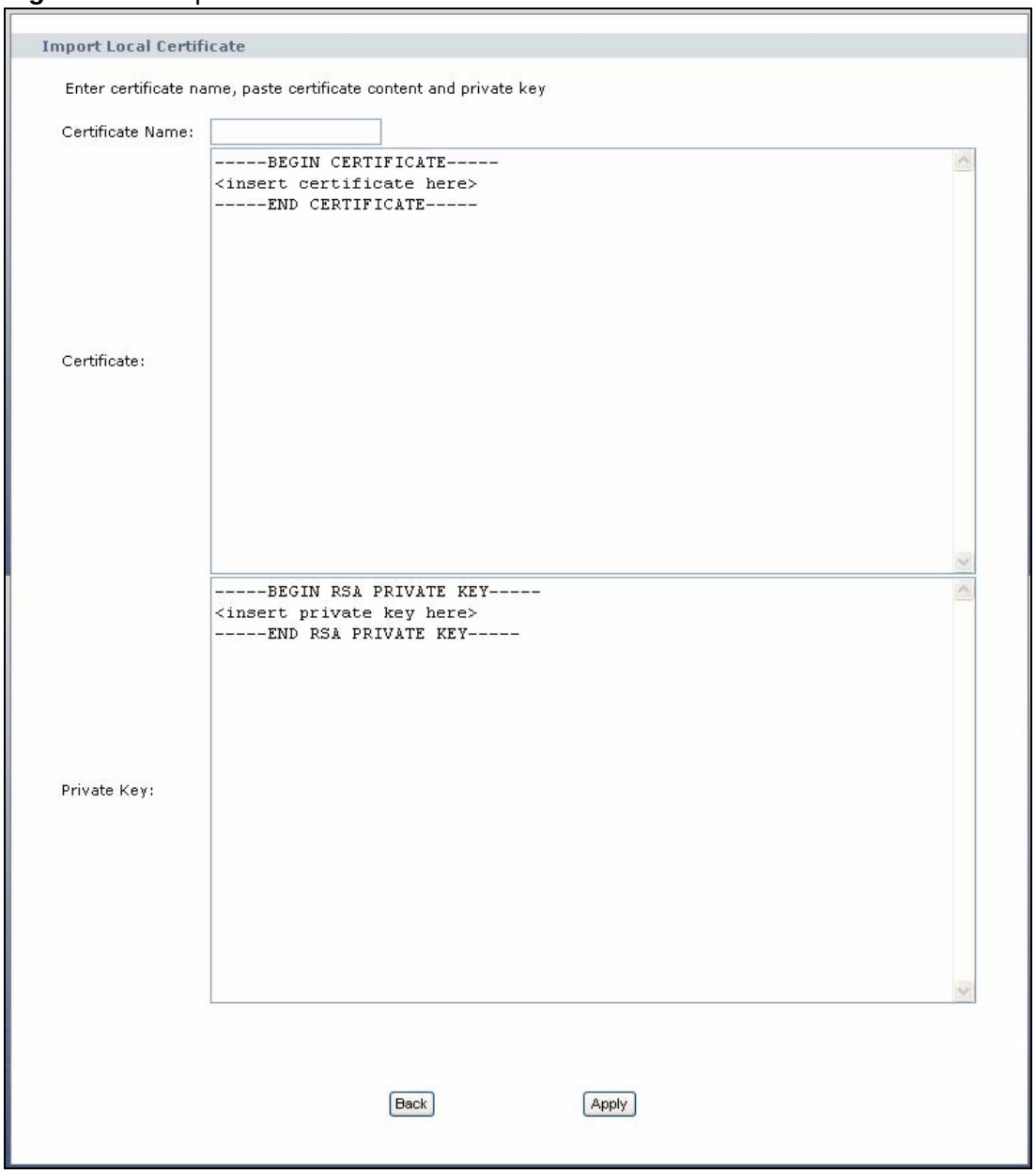


14.3.2 Import Certificate

Click **Security > Certificates > Local Certificates** and then **Import Certificate** to open the **Import Local Certificate** screen. Follow the instructions in this screen to save an existing certificate to the P-2812HNU-51c.

Note: You must remove any spaces from the certificate's filename before you can import it.

Figure 143 Import Local Certificate



The following table describes the labels in this screen.

Table 88 Import Local Certificate

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the P-2812HNU-51c.

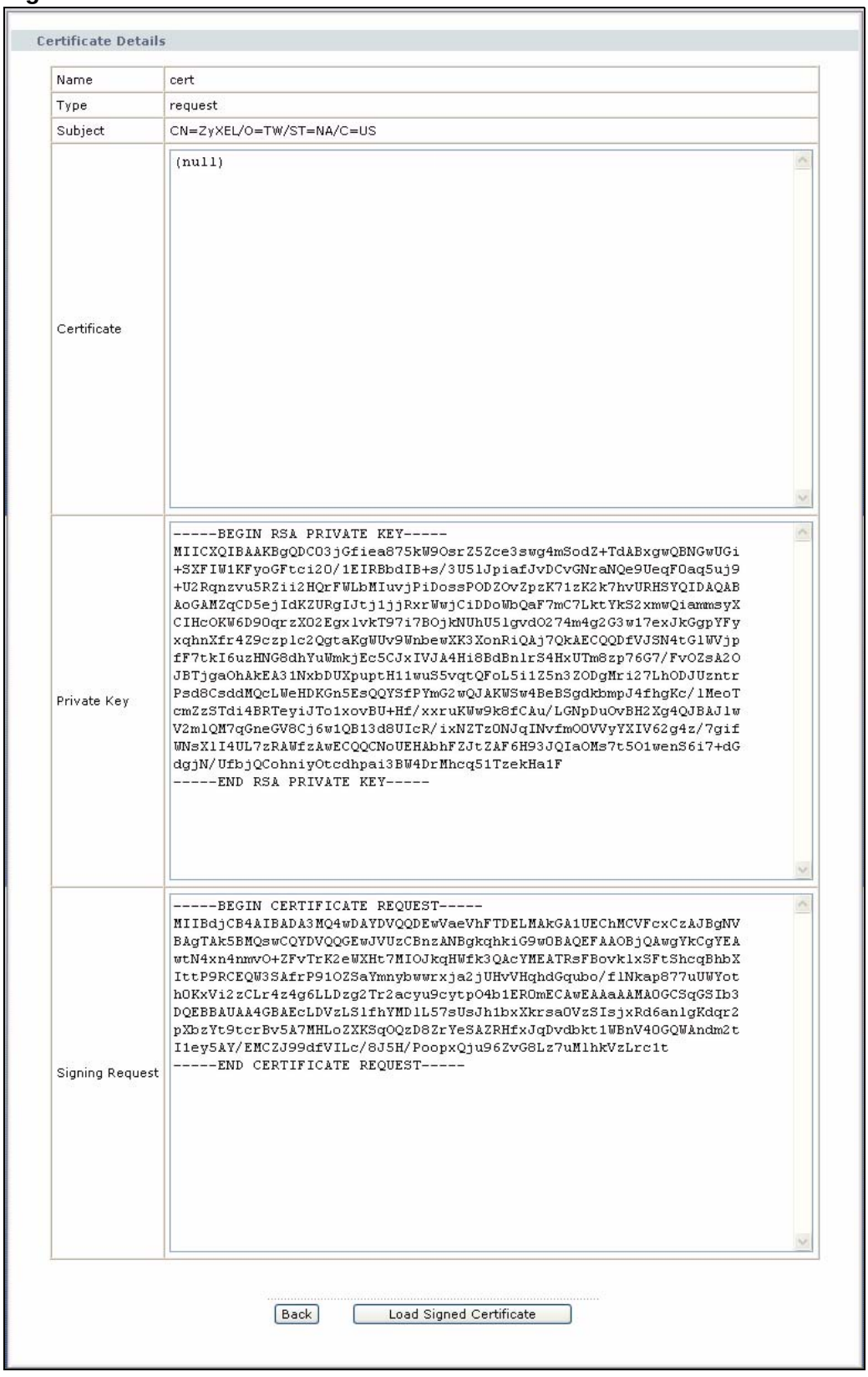
Table 88 Import Local Certificate

LABEL	DESCRIPTION
Private Key	Copy and paste the private key into the text box to store it on the P-2812HNU-51c.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the P-2812HNU-51c.

14.3.3 Certificate Details

Click **Security** > **Certificates** > **Local Certificates** to open the **My Certificates** screen (see Figure 140 on page 282). Click the **View** icon to open the **Certificate Details** screen. Use this screen to view in-depth certificate information and change the certificate's name.

Figure 144 Certificate Details



The following table describes the labels in this screen.

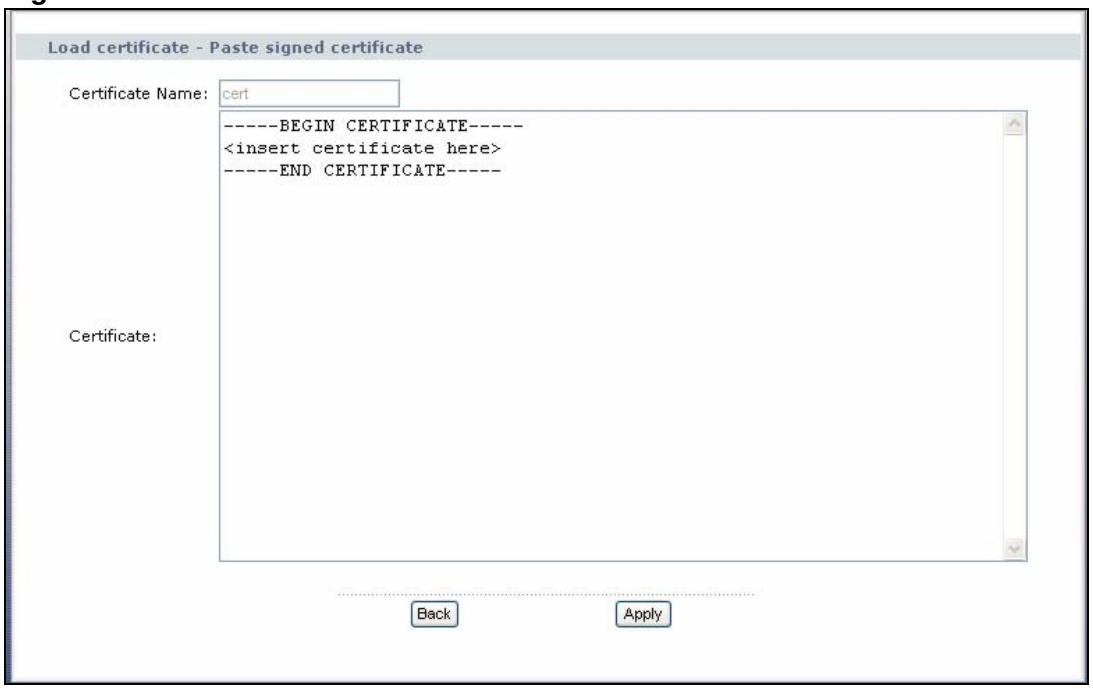
Table 89 Certificate Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Type	This field displays general information about the certificate. **signed** means that a Certification Authority signed the certificate. **request** means this is a certification request.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organization (O), State (ST) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. This displays **null** in a certification request. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Private Key	This read-only text box displays the private key in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the private key into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Signing Request	This read-only text box displays the request information in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. This displays **null** in a signed certificate.
Back	Click **Back** to return to the previous screen.
Load Signed Certificate	This button is available only in a certification request details screen Click this to import a certificate signed by the CA to replace the request.

14.3.4 Load Signed Certificate

Click **Security > Certificates > Local Certificates** and then **Load Signed** or the **Load Signed Certificate** button in the **Certificate Details** screen of a certification request to open the **Load Certificate** screen. Follow the instructions in this screen to save a valid certificate to repalce the request.

Figure 145 Load Certificate



The following table describes the labels in this screen.

Table 90 Load Certificate

LABEL	DESCRIPTION
Certificate Name	This field is read-only and displays the identifying name of this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the P-2812HNU-51c.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the P-2812HNU-51c.

14.4 The Trusted CA Screen

Click **Advanced Setup > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the P-2812HNU-51c to accept as trusted. The P-2812HNU-51c accepts any valid certificate signed by a certification authority on

this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 146 Trusted CA

The following table describes the fields in this screen.

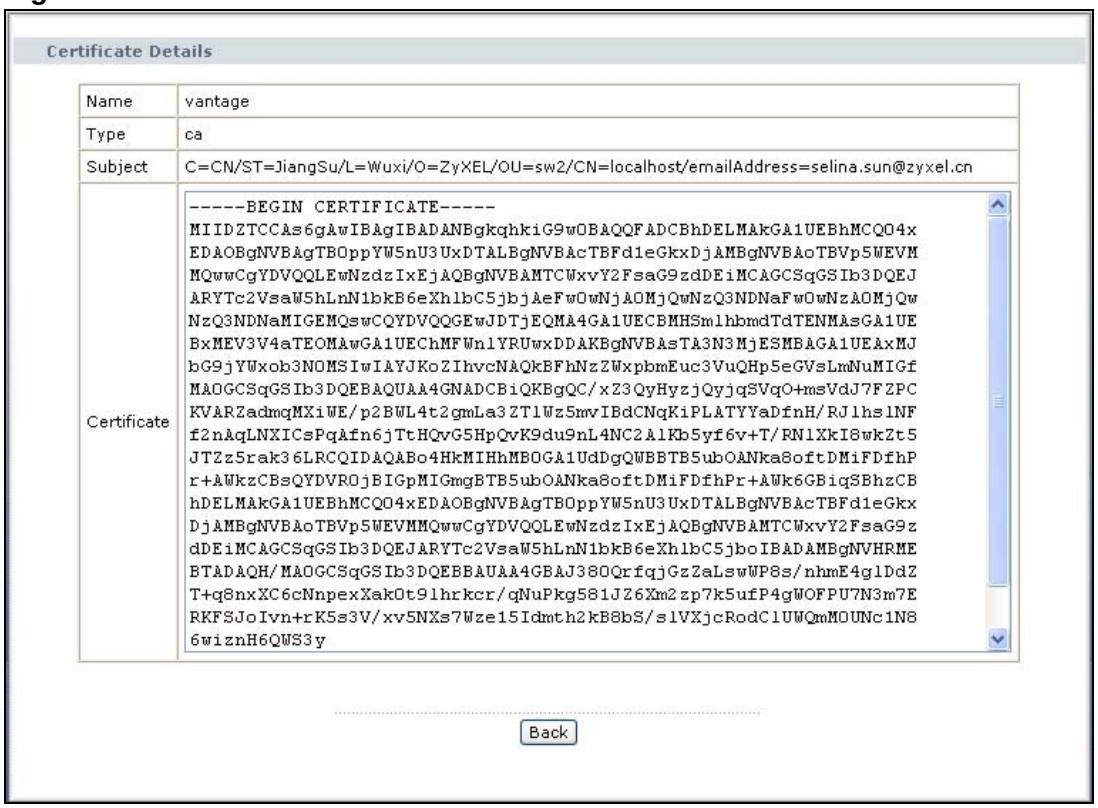
Table 91 Trusted CA

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Action	Click **View** to open a screen with an in-depth list of information about the certificate. Click **Remove** to delete the certificate.
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the P-2812HNU-51c.

14.4.1 View Trusted CA Certificate

Click the **View** button in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate.

Figure 147 Trusted CA: View



The following table describes the fields in this screen.

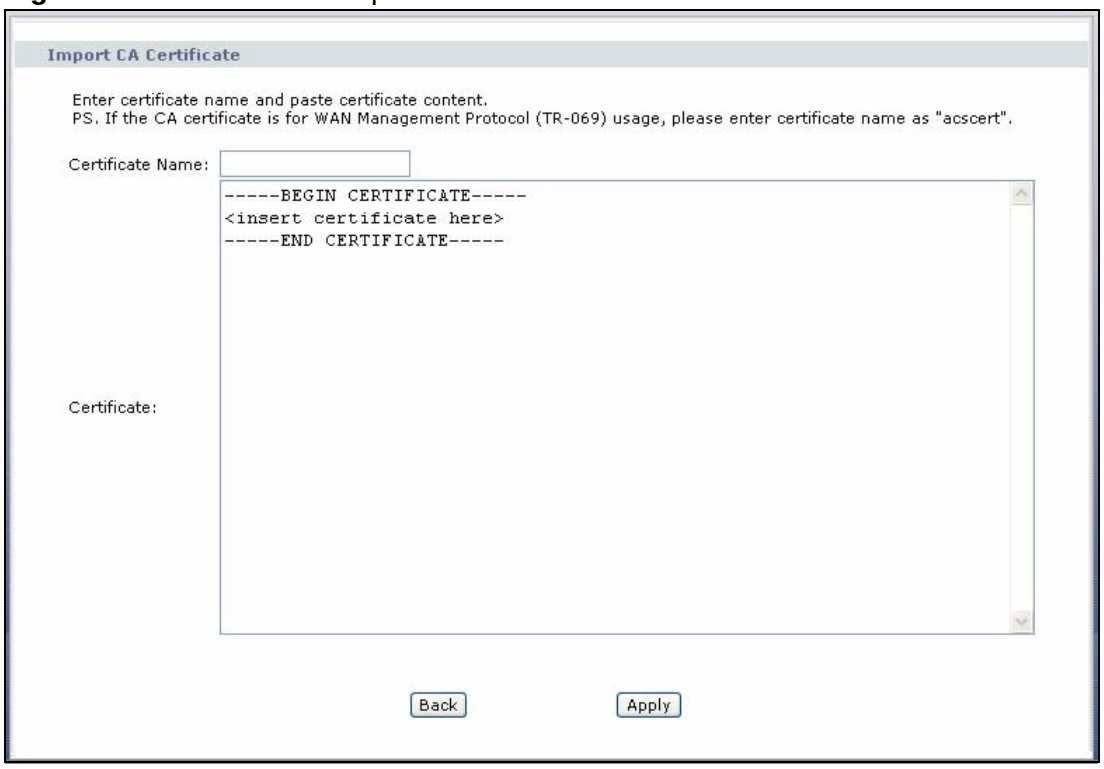
Table 92 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this button to return to the previous screen.

14.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The P-2812HNU-51c trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 148 Trusted CA: Import Certificate


Import CA Certificate
Enter certificate name and paste certificate content.
PS. If the CA certificate is for WAN Management Protocol (TR-069) usage, please enter certificate name as "acscert".
Certificate Name:
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
Certificate:
Back
Apply

The following table describes the fields in this screen.

Table 93 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate Name	Enter the name that identifies this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the P-2812HNU-51c.
Back	Click this button to return to the previous screen.
Apply	Click this button to save your changes back to the P-2812HNU-51c.

15

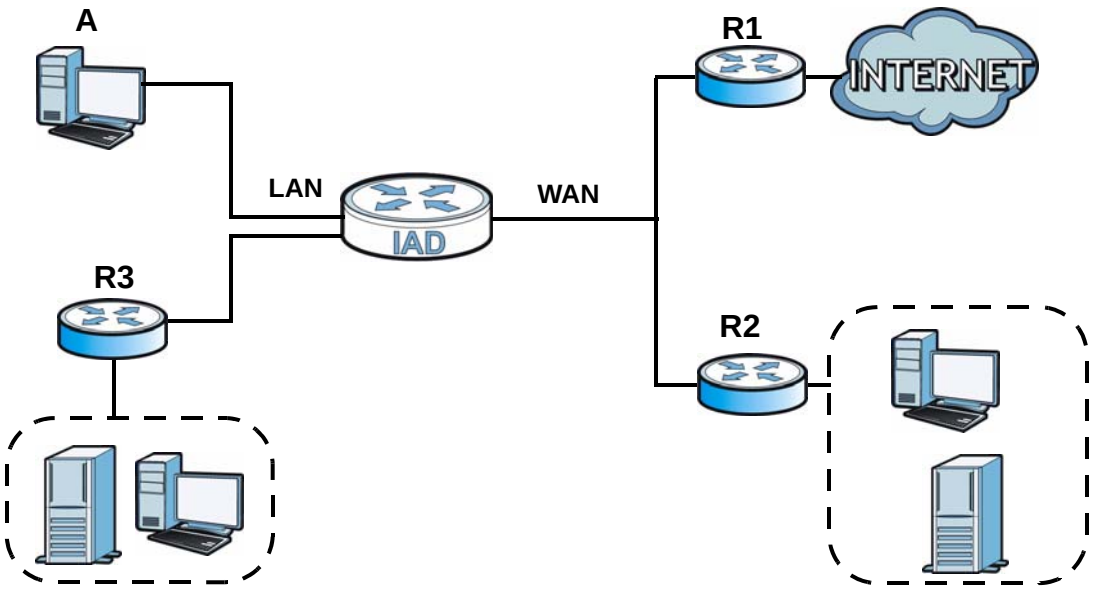
Static Route

15.1 Overview

The P-2812HNU-51c usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the P-2812HNU-51c send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the P-2812HNU-51c's LAN interface. The P-2812HNU-51c routes most traffic from **A** to the Internet through the P-2812HNU-51c's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 149 Example of Static Routing Topology



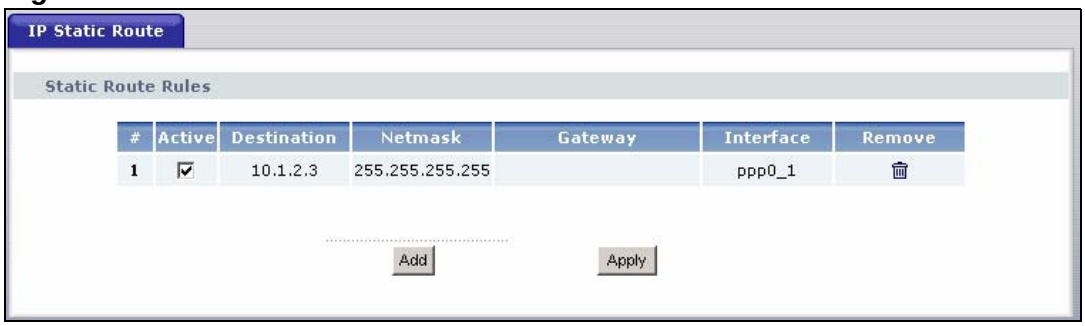
15.1.1 What You Can Do in this Chapter

The **Static Route** screens let you view and configure IP static routes on the P-2812HNU-51c (Section 15.2 on page 294).

15.2 The Static Route Screen

Click **Advanced > Static Route** to open the **Static Route** screen.

Figure 150 Advanced > Static Route



The following table describes the labels in this screen.

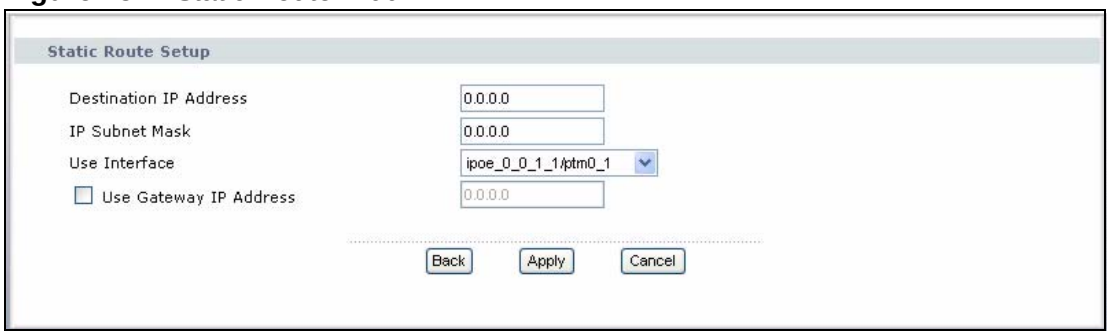
Table 94 Advanced > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Netmask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface through which the traffic is routed.
Remove	Click the icon to remove a static route from the P-2812HNU-51c. A window displays asking you to confirm that you want to delete the route.
Add	Click this to create a new rule.
Apply	Click this to apply your changes to the P-2812HNU-51c.

15.2.1 Static Route Edit

Click the **Add** button in the **Static Route** screen. Use this screen to configure the required information for a static route.

Figure 151 Static Route: Add



The following table describes the labels in this screen.

Table 95 Static Route: Add

LABEL	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **WAN** screens.
Use Gateway IP Address	Select this option and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your P-2812HNU-51c's interface(s). The gateway helps forward packets to their destinations.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16

Policy Forwarding

16.1 Overview

Traditionally, routing is based on the destination address only and the P-2812HNU-51c takes the shortest path to forward a packet. Policy forwarding allows the P-2812HNU-51c to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

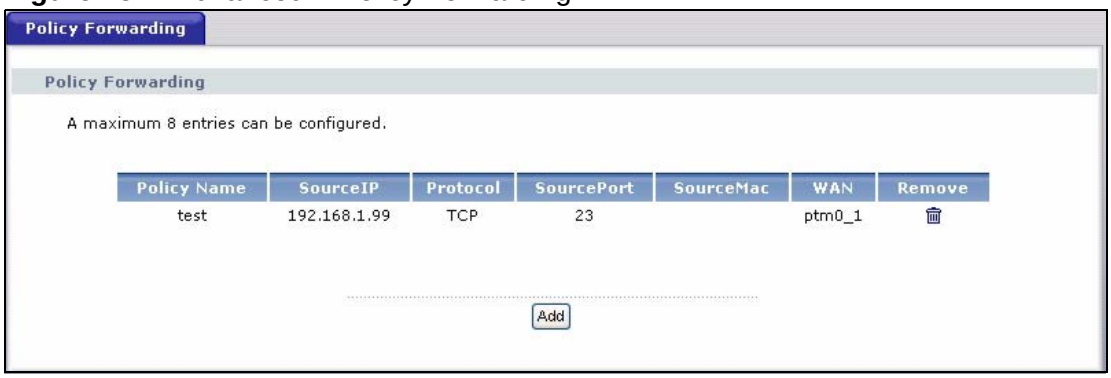
16.1.1 What You Can Do in this Chapter

The **Policy Forwarding** screens let you view and configure routing policies on the P-2812HNU-51c (Section 16.2 on page 297).

16.2 The Static Route Screen

Click **Advanced > Policy Forwarding** to open the **Policy Forwarding** screen.

Figure 152 Advanced > Policy Forwarding



The following table describes the labels in this screen.

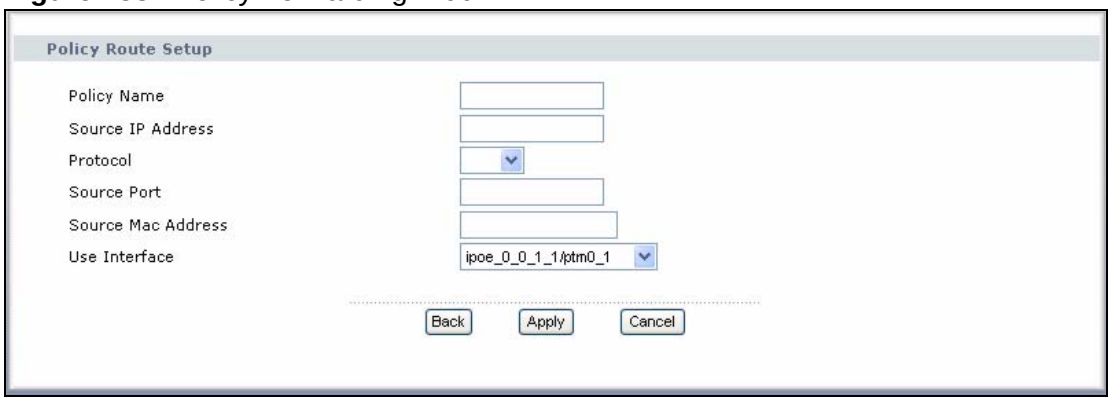
Table 96 Advanced > Policy Forwarding

LABEL	DESCRIPTION
Policy Name	This is the name of the rule.
SourceIP	This is the source IP address.
Protocol	This is the transport layer protocol.
SourcePort	This is the source port number.
SourceMAC	This is the source MAC address.
Interface	This is the WAN interface through which the traffic is routed.
Remove	Click the icon to remove a rule from the P-2812HNU-51c. A window displays asking you to confirm that you want to delete the rule.
Add	Click this to create a new rule.

16.2.1 Policy Forwarding Setup

Click the **Add** button in the **Policy Forwarding** screen. Use this screen to configure the required information for a policy route.

Figure 153 Policy Forwarding: Add



The following table describes the labels in this screen.

Table 97 Policy Forwarding: Add

LABEL	DESCRIPTION
Policy Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces.
Source IP Address	Enter the source IP address.
Protocol	Select the transport layer protocol (**TCP** or **UDP**).
Source Port	Enter the source port number.
Source Mac Address	Enter the source MAC address.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **WAN** screens.

Table 97 Policy Forwarding: Add

LABEL	DESCRIPTION
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17

DNS Route

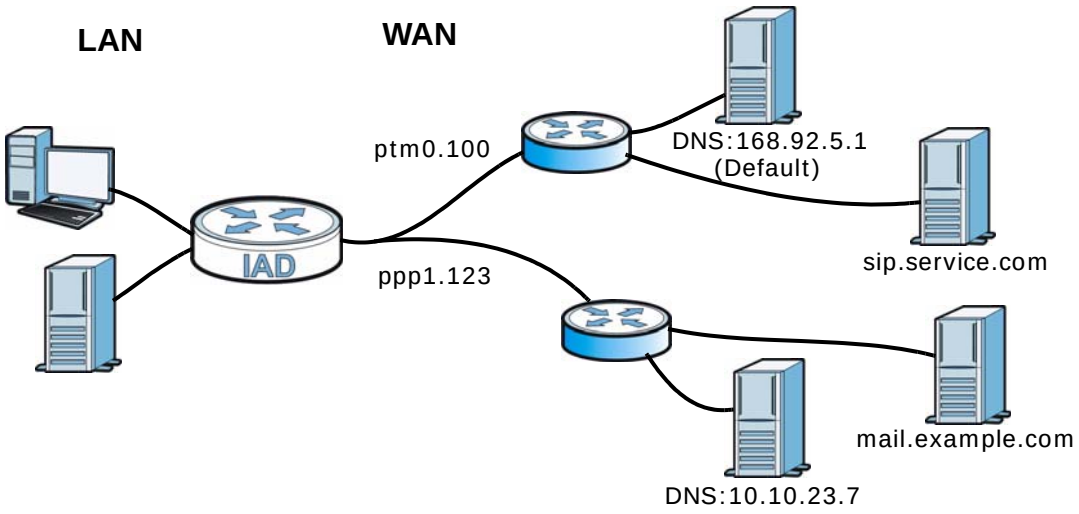
17.1 Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS server(s), each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). The P-2812HNU-51c uses a system DNS server (in the order you specify in the **WAN** > **Internet Connection** screen) to resolve domain names that do not match any DNS routing entry. After the P-2812HNU-51c receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

In the following example, the DNS server 168.92.5.1 obtained from the WAN interface ptm0.100 is set to be the system DNS server. The DNS server 10.10.23.7 is obtained from the WAN interface ppp1.123. You configure a DNS route for *example.com to have the P-2812HNU-51c forward DNS requests for the domain name mail.example.com through the WAN interface ppp1.123 to the DNS server 10.10.23.7.

Figure 154 Example of DNS Routing Topology



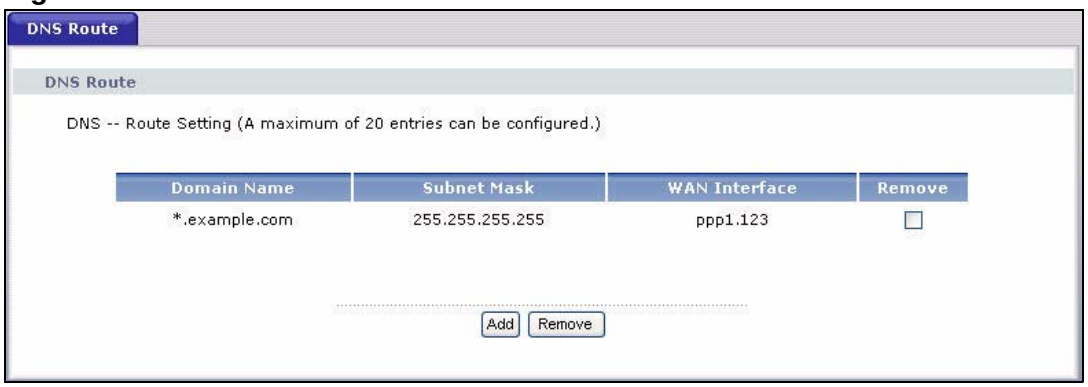
17.1.1 What You Can Do in this Chapter

The **DNS Route** screens let you view and configure DNS routes on the P-2812HNU-51c (Section 17.2 on page 302).

17.2 The DNS Route Screen

Click **Advanced > DNS Route** to open the **DNS Route** screen.

Figure 155 Advanced > DNS Route



The following table describes the labels in this screen.

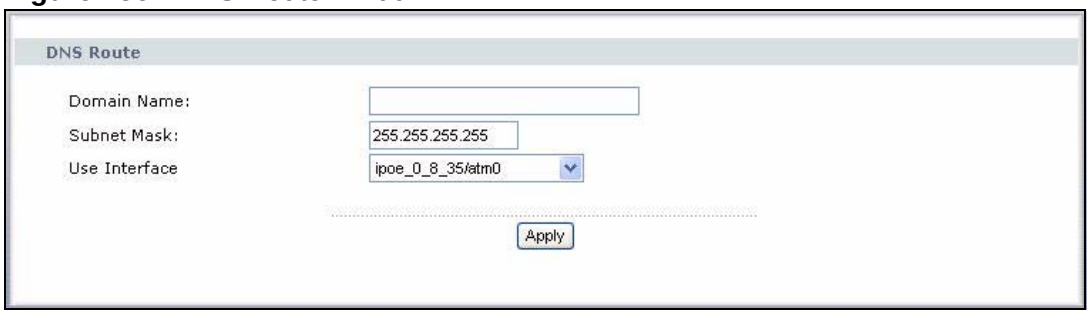
Table 98 Advanced > DNS Route

LABEL	DESCRIPTION
Domain Name	This is the domain name to which the DNS route applies.
Subnet Mask	This is the network subnet mask for the resolved IP address.
WAN Interface	This is the WAN interface through which the matched DNS request is routed.
Remove	Select the check box of the entry you want to delete and click the **Remove** button.
Add	Click this button to create a new entry.
Remove	Click this button to delete the selected entry(ies).

17.2.1 DNS Route Edit

Click the **Add** button in the **DNS Route** screen. Use this screen to configure the required information for a DNS route.

Figure 156 DNS Route > Add



The following table describes the labels in this screen.

Table 99 DNS Route > Add

LABEL	DESCRIPTION
Domain Name	Enter the domain name you want to resolve. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The P-2812HNU-51c forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
IP Subnet Mask	Enter the subnet mask for the resolved IP address. The subnet mask specifies the network number portion of an IP address. This is to specify the size of the network number, which determines the maximum number of possible resolved IP addresses for the same domain name.
Use Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interface(s) already configured in the **WAN** screens.
Apply	Click this button to save your changes and return to the previous screen.

18 RIP

18.1 Overview

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

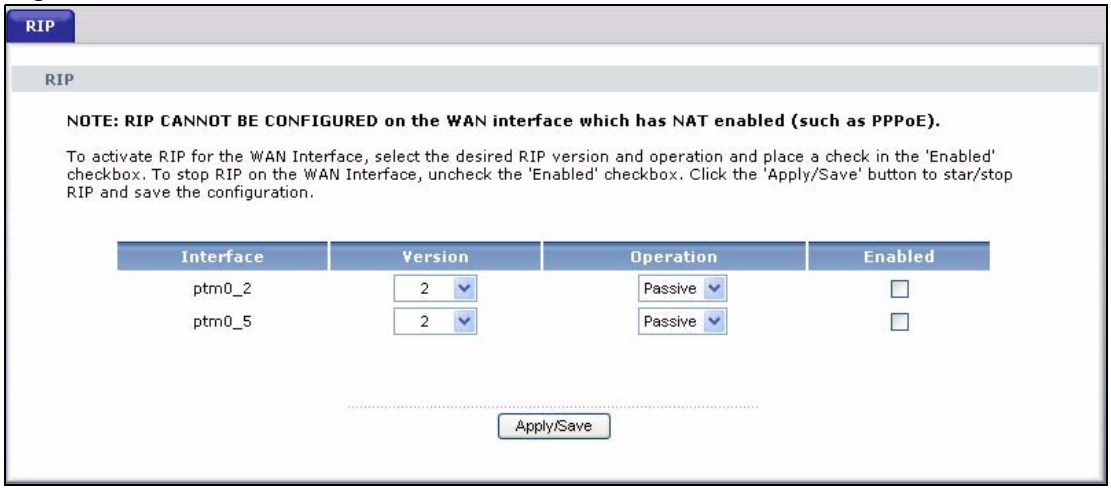
18.1.1 What You Can Do in this Chapter

The **RIP** screen lets you set up RIP settings on the P-2812HNU-51c (Section 18.2 on page 305).

18.2 The RIP Screen

Click **Advanced > RIP** to open the **RIP** screen.

Figure 157 Advanced > RIP


RIP
RIP
NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).
To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.
Interface
Version
Operation
Enabled
ptm0_2
2
Passive
ptm0_5
2
Passive
Apply/Save

The following table describes the labels in this screen.

Table 100 Advanced > RIP

LABEL	DESCRIPTION
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the P-2812HNU-51c sends (it recognizes both formats when receiving). RIP version **1** is universally supported but RIP version **2** carries more information. RIP version **1** is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select **Passive** to have the P-2812HNU-51c update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select **Active** to have the P-2812HNU-51c advertise its route information and also listen for routing updates from neighboring routers.
Enabled	Select the check box to activate the settings.
Apply/Save	Click **Apply/Save** to save your changes back to the P-2812HNU-51c.

19

Quality of Service (QoS)

19.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the P-2812HNU-51c to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

1 Configure classifiers to sort traffic into different flows.

2 Assign priority and define actions to be performed for a classified traffic flow.

The P-2812HNU-51c assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

This chapter contains information about configuring QoS and editing classifiers.

19.1.1 What You Can Do in this Chapter

- The **General** screen lets you lets you enable or disable QoS, set the bandwidth, and allow the P-2812HNU-51c to automatically assign priority to upstream traffic according to the IEEE 802.1p priority level, IP precedence or packet length (Section 19.3 on page 309).
- The **Queue Setup** screen lets you lets you configure QoS queue assignment (Section 19.4 on page 311).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers (Section 19.5 on page 313).

- The **Policer Setup** screen lets you add, edit or delete QoS policers (Section 19.5 on page 313).
- The **Monitor** screen lets you view the P-2812HNU-51c's QoS-related packet statistics (Section 19.7 on page 323).

19.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

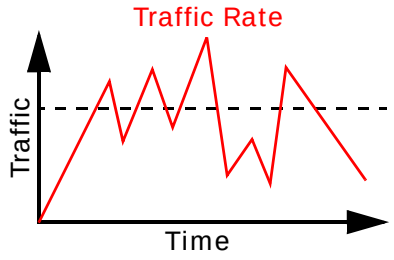
Tagging and Marking

In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

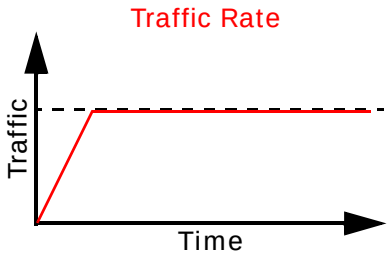
Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or

queues). Your P-2812HNU-51c uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



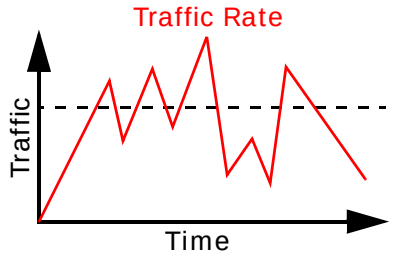
(Before Traffic Shaping)



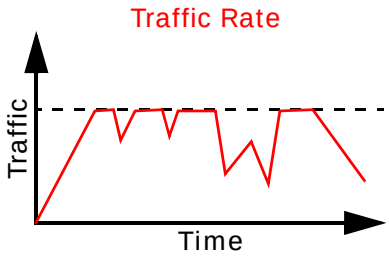
(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



(Before Traffic Policing)



(After Traffic Policing)

The P-2812HNU-51c supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 19.8 on page 324 for more information on each metering algorithm.

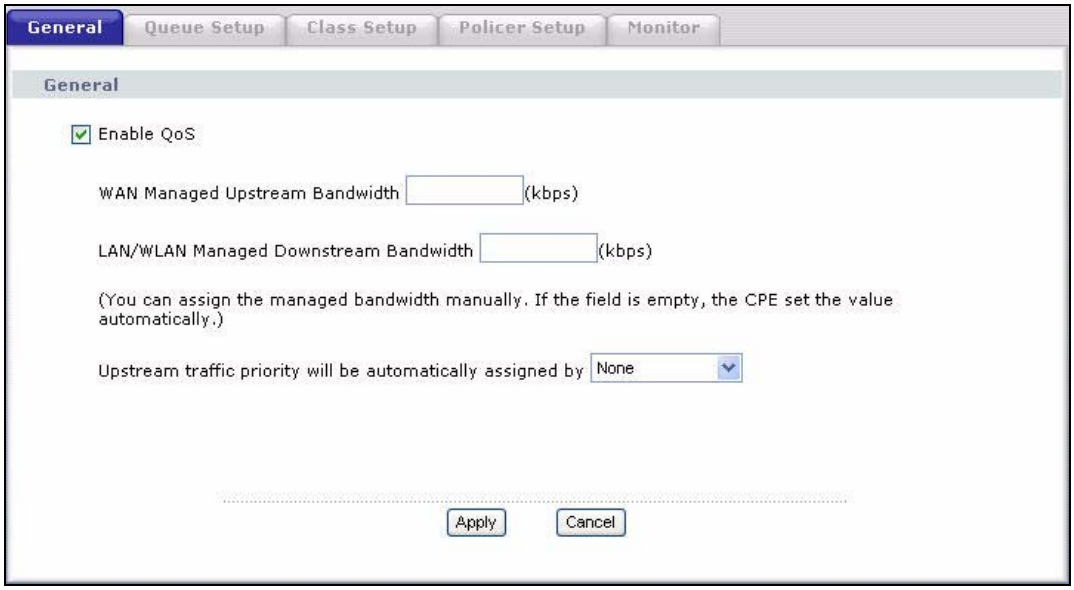
19.3 The Quality of Service General Screen

Click **Advanced Setup** > **Quality of Service** to open the screen as shown next.

Use this screen to enable or disable QoS, set the bandwidth, and select to have the P-2812HNU-51c automatically assign priority to upstream traffic according to

the IEEE 802.1p priority level, IP precedence or packet length. See Section 19.1 on page 307 for more information.

Figure 158 QoS General



The following table describes the labels in this screen.

Table 101 QoS General

LABEL	DESCRIPTION
Enable QoS	Select the check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can set this number higher than the interface's actual transmission speed. The P-2812HNU-51c uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed. You can also set this number lower than the interface's actual transmission speed. This will cause the P-2812HNU-51c to not use some of the interface's available bandwidth. If you leave this field blank, the P-2812HNU-51c automatically sets this number to be 95% of the DSL port's actual upstream transmission speed.
LAN/WLAN Managed Downstream Bandwidth	Enter the amount of downstream bandwidth for the LAN/WLAN interface that you want to allocate using QoS.

Table 101 QoS General

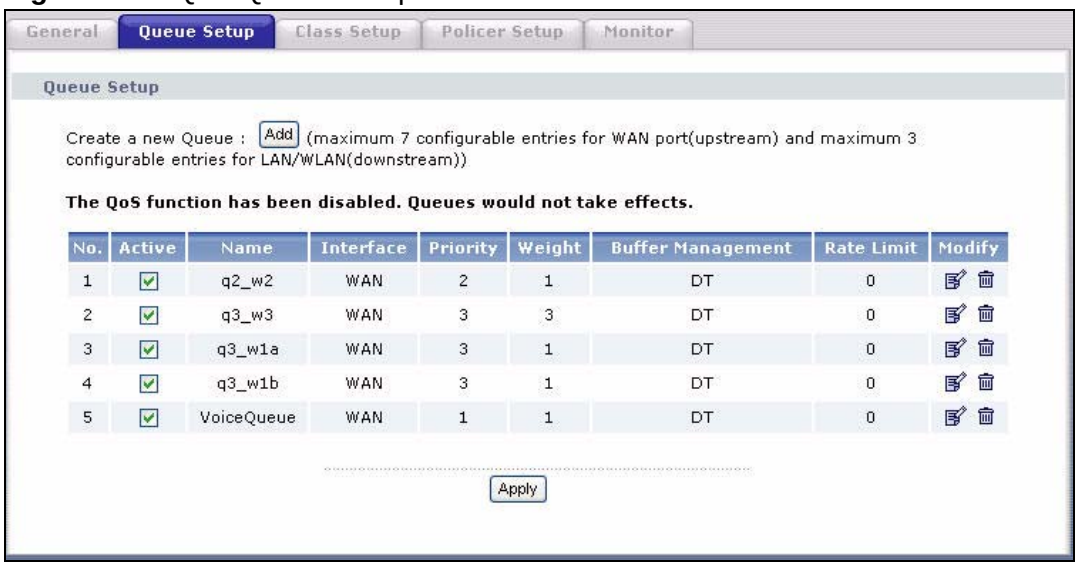
LABEL	DESCRIPTION
Upstream traffic priority will be automatically assigned by	These fields are ignored if upstream traffic matches a class you configured in the **Class Setup** screen. If you select **Ethernet Priority**, **IP Precedence** or **Packet Length** and traffic does not match a class configured in the **Class Setup** screen, the P-2812HNU-51c assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence or packet length. See Section 19.8 on page 324 for more information. If you select **None**, traffic which does not match a class is mapped to the default queue with the lowest priority.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

19.4 The Queue Setup Screen

Click **QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queues for egress traffic shaping.

Figure 159 QoS Queue Setup


General
Queue Setup
Class Setup
Policer Setup
Monitor
Queue Setup
Create a new Queue : Add (maximum 7 configurable entries for WAN port(upstream) and maximum 3 configurable entries for LAN/WLAN(downstream))
The QoS function has been disabled. Queues would not take effects.
No. Active Name Interface Priority Weight Buffer Management Rate Limit Modify
1 q2_w2 WAN 2 1 DT 0
2 q3_w3 WAN 3 3 DT 0
3 q3_w1a WAN 3 1 DT 0
4 q3_w1b WAN 3 1 DT 0
5 VoiceQueue WAN 1 1 DT 0
Apply

The following table describes the labels in this screen.

Table 102 QoS Queue Setup

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
No.	This is the index number of this entry.
Active	Select the check box to enable the queue.

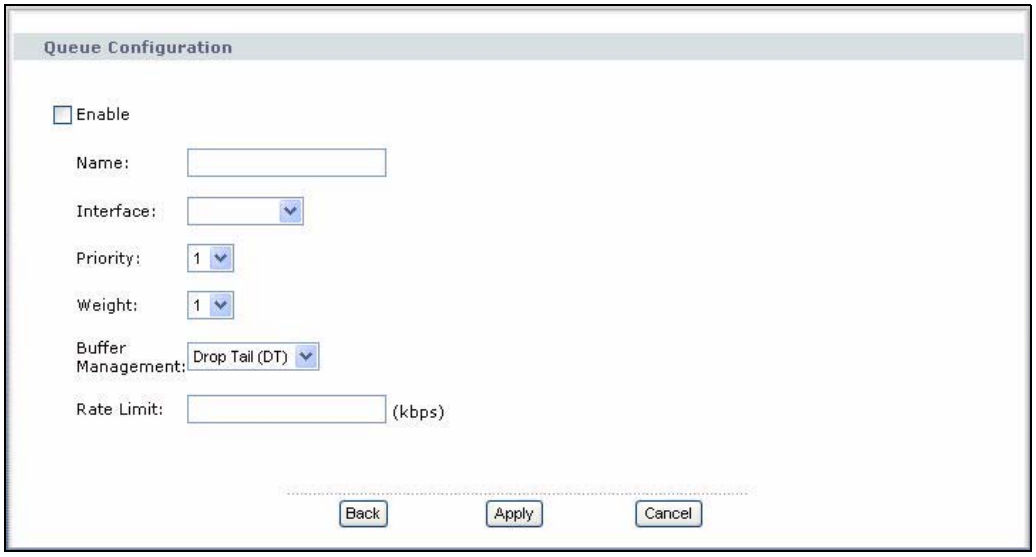
Table 102 QoS Queue Setup

LABEL	DESCRIPTION
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the P-2812HNU-51c's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the P-2812HNU-51c should handle packets when it receives too many (network congestion).
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue. **0** means no rate limit.
Modify	Click the **Edit** icon to go to the screen where you can edit the queue. Click the **Remove** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.

19.4.1 Adding a QoS Queue

Click the **Add** button or the edit icon in the **Queue Setup** screen to configure a queue.

Figure 160 QoS Queue Setup: Add



The following table describes the labels in this screen.

Table 103 QoS Queue Setup: Add

LABEL	DESCRIPTION
Enable	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied.
Priority	Select the priority level (from 1 to 4) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the P-2812HNU-51c divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays **Drop Tail (DT)**. **Drop Tail (DT)** is a simple queue management algorithm that allows the P-2812HNU-51c buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in kbps) allowed for traffic on this queue. **0** means no rate limit.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

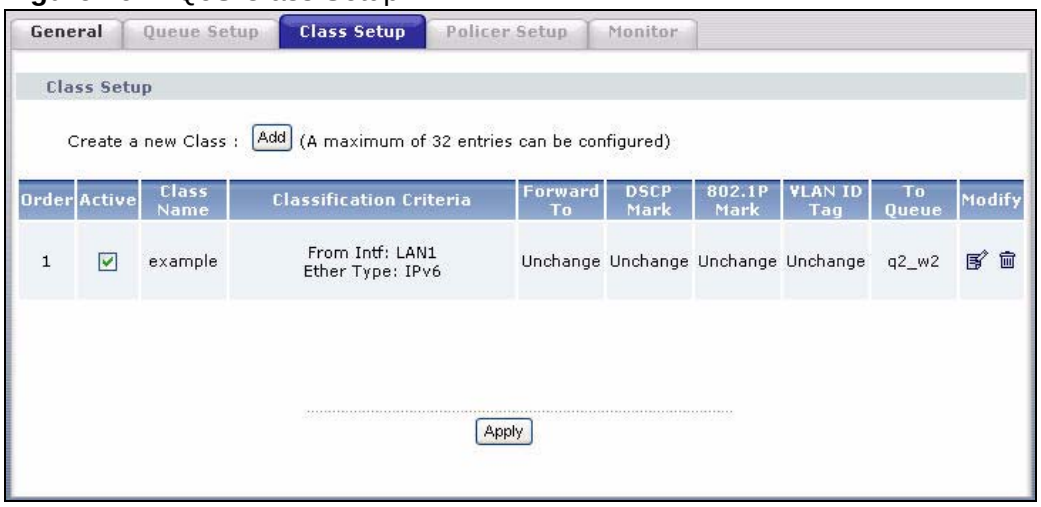
19.5 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the P-2812HNU-51c forwards out through the LAN/WLAN or WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **QoS > Class Setup** to open the following screen.

Figure 161 QoS Class Setup



The following table describes the labels in this screen.

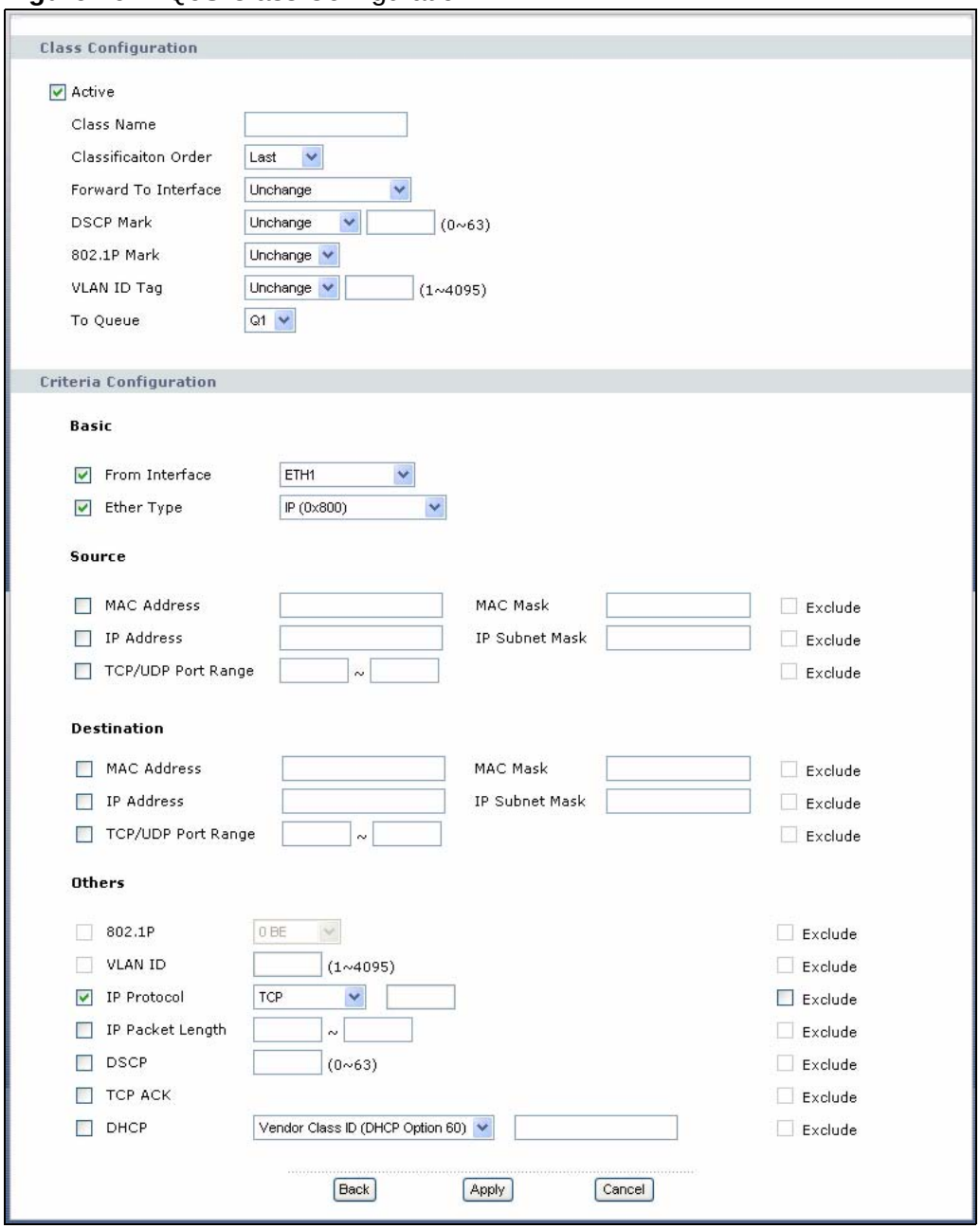
Table 104 QoS Class Setup

LABEL	DESCRIPTION
Add	Click this button to create a new classifier.
Order	This field displays the index number of the classifier.
Active	Select the check box to enable the classifier.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
Forward To	This is the interface through which traffic that matches this classifier is forwarded out.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to go to the screen where you can edit the classifier. Click the **Remove** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.

19.5.1 QoS Class Edit

Click the **Add** button or the **Edit** icon in the **Class Setup** screen to configure a classifier.

Figure 162 QoS Class Configuration



The following table describes the labels in this screen.

Table 105 QoS Class Configuration

LABEL	DESCRIPTION
Class Configuration	
Active	Select to enable or disable this classifier.
Class Name	Enter a descriptive name of up to 20 printable English keyboard characters, including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the P-2812HNU-51c forward traffic of this class according to the default routing table. If traffic of this class comes from a WAN interface and is in a queue that forwards traffic through the LAN/WLAN interface, the P-2812HNU-51c ignores the setting here.
DSCP Mark	This field is available only when you select the **Ether Type** check box. If you select **Mark**, enter a DSCP value with which the P-2812HNU-51c replaces the DSCP field in the packets. If you select **Auto Mapping** and there is a VLAN tag carried in the matched packets, the P-2812HNU-51c will replace the IP ToS field with the 802.1p priority field. If you select **Unchange**, the P-2812HNU-51c keep the DSCP field in the packets.
802.1p Mark	Select a priority level with which the P-2812HNU-51c replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the P-2812HNU-51c keep the 802.1p priority field in the packets.
VLAN ID Tag	If you select **Remark**, enter a VLAN ID number (between 1 and 4095) with which the P-2812HNU-51c replaces the VLAN ID of the frames. If you select **Remove**, the P-2812HNU-51c deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the P-2812HNU-51c treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the P-2812HNU-51c keep the VLAN ID in the packets.
To Queue	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Criteria Configuration Use the following fields to configure the criteria for traffic classification.	
Basic	

Table 105 QoS Class Configuration (continued)

LABEL	DESCRIPTION
From Interface	Select from which LAN, WLAN or WAN interface traffic of this class should come.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **8021Q**, you can configure an 802.1p priority level and VLAN ID in the **Others** section.
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
TCP/UDP Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.
TCP/UDP Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.

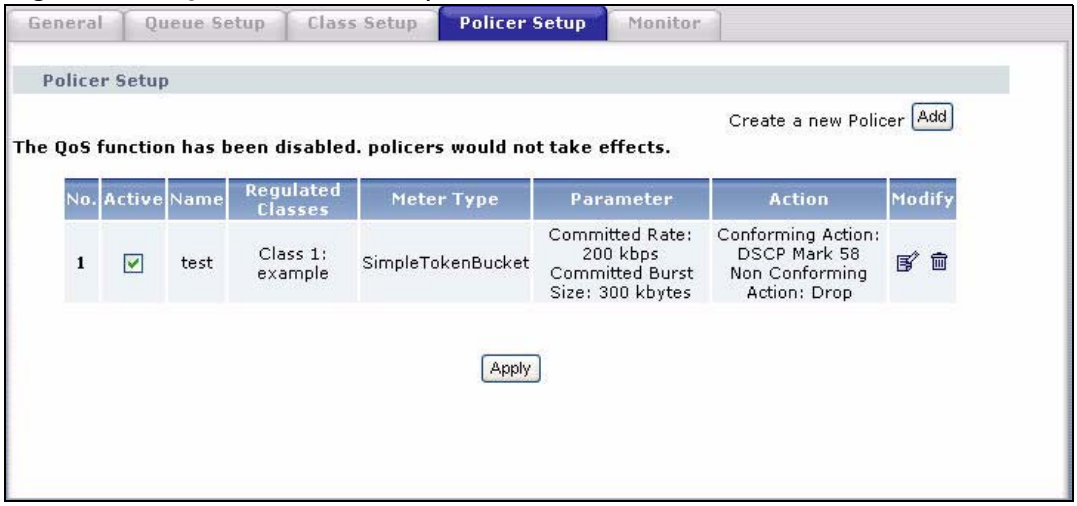
Table 105 QoS Class Configuration (continued)

LABEL	DESCRIPTION
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number between 1 and 4095.
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP**, **UDP**, **ICMP** or **IGMP**. If you select **User defined**, enter the protocol (service type) number.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
DHCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. If you select **User Class ID (DHCP Option 77)**, enter a string that identifies the user's category or application type in the matched DHCP packets.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

19.6 The QoS Policer Setup Screen

Use this screen to configure QoS policers that allow you to limit the transmission rate of incoming traffic. Click **Advanced > QoS > Policer Setup**. The screen appears as shown.

Figure 163 QoS > Policer Setup



The following table describes the labels in this screen.

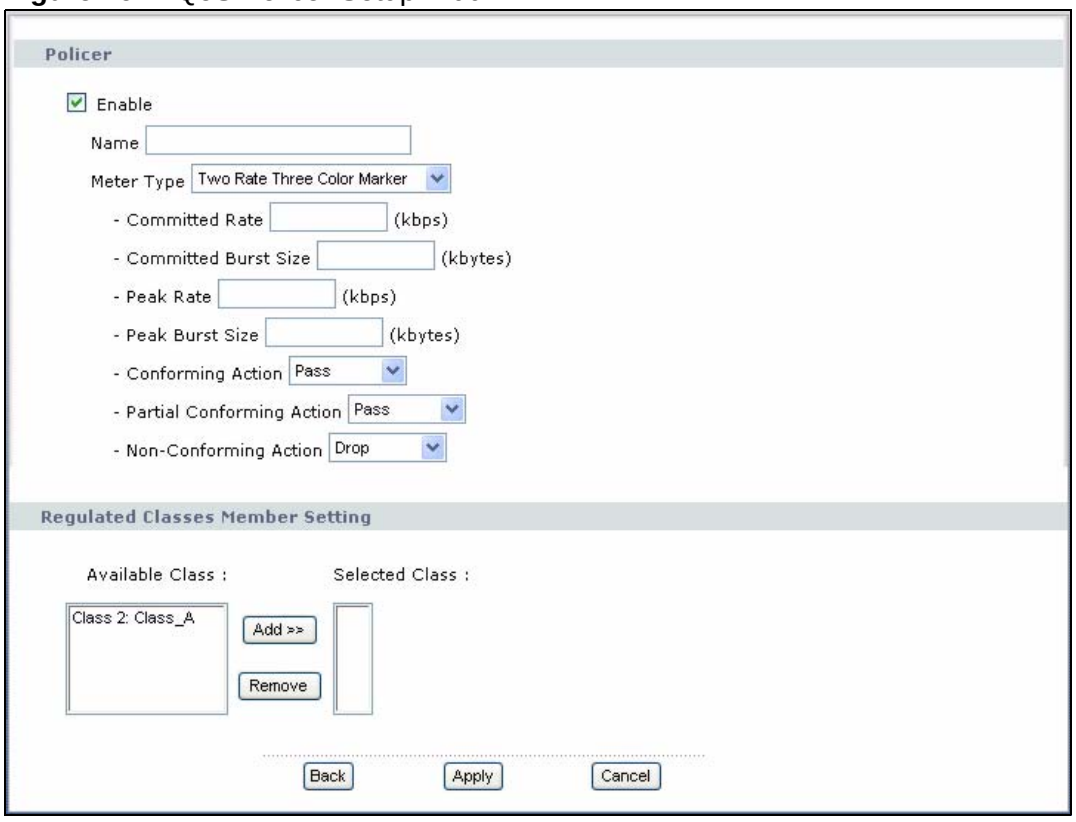
Table 106 QoS > Policer Setup

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
No.	This is the index number of this entry.
Active	Select the check box to enable the policer.
Name	This field displays the descriptive name of this policer.
Regulated Classes	This field displays the name of a QoS classifier
Meter Type	This field displays the type of QoS metering algorithm used in this policer.
Parameter	This field displays the parameters configured for the metering algorithm in the policer.
Action	This field displays the actions taken on the matched traffic.
Modify	Click the **Edit** icon to go to the screen where you can edit the policer. Click the **Remove** icon to delete an existing policer. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.

19.6.1 Adding a QoS Policer

Click the **Add** button or the edit icon in the **Policer Setup** screen to configure a policer.

Figure 164 QoS Policer Setup: Add



The following table describes the labels in this screen.

Table 107 QoS Policer Setup: Add

LABEL	DESCRIPTION
Enable	Select to enable or disable this policer.
Name	Enter the descriptive name of this policer.

Table 107 QoS Policer Setup: Add

LABEL	DESCRIPTION
Meter Type	Select a traffic metering algorithm used in this policer. The **Simple Token Bucket** algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size. The **Single Rate Three Color Marker** (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS). The **Two Rate Three Color Marker** (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR). See Section 19.8 on page 324 for more information.
Committed Rate	Specify the guaranteed rate at which packets are admitted to the network. This is to specify how many bytes of tokens are added to a bucket every second.
Committed Burst Size	Specify the guaranteed amount of bytes that are admitted at the committed rate. This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Excess Burst Size	Specify the additional amount of bytes that are admitted at the committed rate besides the committed burst size. This is the maximum size of the second token bucket in the srTCM.
Peak Rate	Specify the maximum rate at which packets are admitted to the network. The peak rate should be greater than or equal to the committed rate. This is to specify how many bytes of tokens are added to the second bucket every second in the trTCM.
Peak Burst Size	Specify the maximum amount of bytes that are admitted at the committed rate. This is the maximum size of the second token bucket in the trTCM.
Conforming Action	Specify the action that the P-2812HNU-51c takes on green-marked packets. Select **Pass** to forward the packets. Select **DSCP Mark** to assign a specified DSCP number (between 0 and 63) to the packets and forward them. The packets are dropped if there is congestion on the network.
Partial Conforming Action	Specify the action that the P-2812HNU-51c takes on yellow-marked packets. Select **Pass** to forward the packets. Select **Drop** to discard the packets. Select **DSCP Mark** to assign a specified DSCP number (between 0 and 63) to the packets and forward them. The packets are dropped if there is congestion on the network.

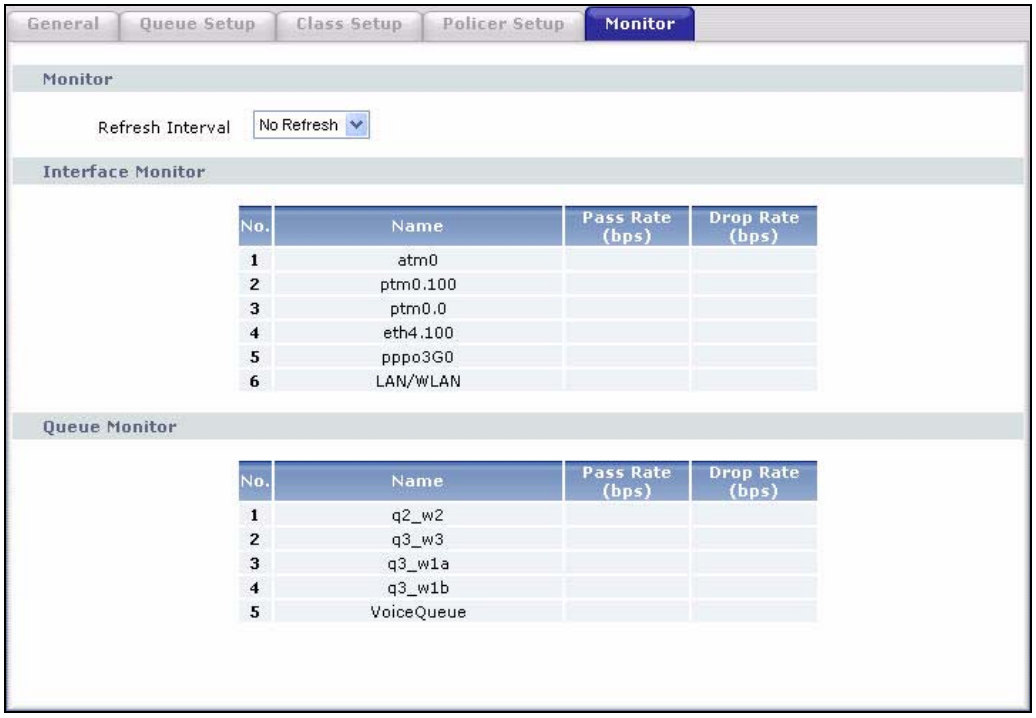
Table 107 QoS Policer Setup: Add

LABEL	DESCRIPTION
Non-Conforming Action	Specify the action that the P-2812HNU-51c takes on red-marked packets. Select **Drop** to discard the packets. Select **DSCP Mark** to assign a specified DSCP number (between 0 and 63) to the packets and forward them. The packets are dropped if there is congestion on the network.
Regulated Classes Member Setting	
Available Class Selected Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier. Highlight a QoS classifier in the **Available Class** box and use the **Add >>** button to move it to the **Selected Class** box. To remove a QoS classifier from the **Selected Class** box, select it and use the **Remove** button.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

19.7 The QoS Monitor Screen

To view the P-2812HNU-51c's QoS packet statistics, click **Advanced > QoS > Monitor**. The screen appears as shown.

Figure 165 QoS > Monitor



The following table describes the labels in this screen.

Table 108 QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the P-2812HNU-51c to update this screen. Select **No Refresh** to stop refreshing statistics.
Interface Monitor	
No.	This is the index number of the entry.
Name	This shows the name of the WAN or LAN/WLAN interface on the P-2812HNU-51c.
Pass	This shows the transmission rate of packets which are forwarded to this interface and transmitted successfully.
Drop	This shows the transmission rate of packets which are forwarded to this interface and dropped.
Queue Monitor	
No.	This is the index number of the entry.
Name	This shows the name of the queue.

Table 108 QoS > Monitor (continued)

LABEL	DESCRIPTION
Pass	This shows the transmission rate of packets which are assigned to this queue and transmitted successfully.
Drop	This shows the transmission rate of packets which are assigned to this queue and dropped.

19.8 Technical Reference

The following section contains additional technical information about the P-2812HNU-51c features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 109 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the P-2812HNU-51c, the P-2812HNU-51c can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the P-2812HNU-51c. On the P-2812HNU-51c, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 110 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size, so the bucket can hold up to *b* tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the P-2812HNU-51c stops transmitting until enough tokens are generated.
- If not enough tokens are available, the P-2812HNU-51c treats the packet in either one of the following ways:

  In traffic shaping:

  - Holds it in the queue until enough tokens are available in the bucket.

  In traffic policing:

  - Drops it.
  - Transmits it but adds a DSCP mark. The P-2812HNU-51c may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the P-2812HNU-51c checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the P-2812HNU-51c checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

20

Dynamic DNS Setup

20.1 Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

20.1.1 What You Can Do in this Chapter

Use the **Dynamic DNS** screen (Section 20.3 on page 330) to enable DDNS and configure the DDNS settings on the P-2812HNU-51c.

20.2 What You Need To Know

DYNDNS Wildcard

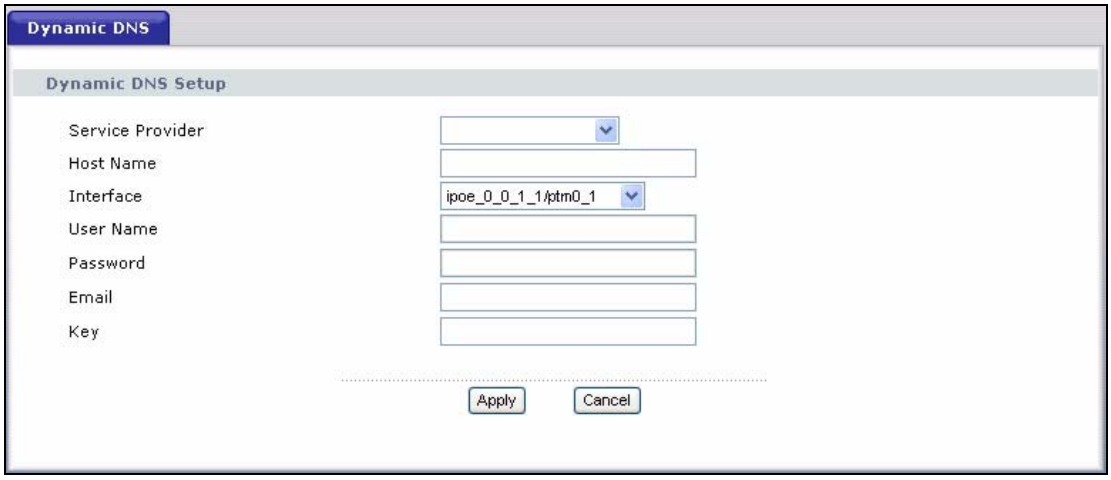
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

20.3 The Dynamic DNS Screen

To change your P-2812HNU-51c's DDNS, click **Advanced > Dynamic DNS**. The screen appears as shown.

Figure 166 Advanced > Dynamic DNS



The following table describes the fields in this screen.

Table 111 Advanced > Dynamic DNS

LABEL	DESCRIPTION
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your P-2812HNU-51c by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Interface	Select the WAN interface to use for updating the IP address of the domain name.
User Name	Type your user name.
Password	Type the password assigned to you.
Email	If you select **TZO** in the **Service Provider** field, enter the user name you used to register for this service.
Key	If you select **TZO** in the **Service Provider** field, enter the password you used to register for this service.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21

Remote Management

21.1 Overview

This chapter explains how to configure the remote management and access control settings on the P-2812HNU-51c.

21.1.1 What You Can Do in this Chapter

- The **TR-069** screen lets you configure the P-2812HNU-51c's TR-069 auto-configuration settings (Section 21.3 on page 333).
- The **TR-064** screen lets you enable management via TR-064 on the P-2812HNU-51c (Section 21.3 on page 333).
- The **SNMP** screen lets you configure your SNMP settings (Section 21.4 on page 334).
- The **Service Control** screens let you configure through which interface(s) users can use which service(s) to manage the P-2812HNU-51c (Section 21.5 on page 336).
- The **IP Address** screens let you configure from which IP address(es) users can use a service to manage the P-2812HNU-51c (Section 21.6 on page 337).

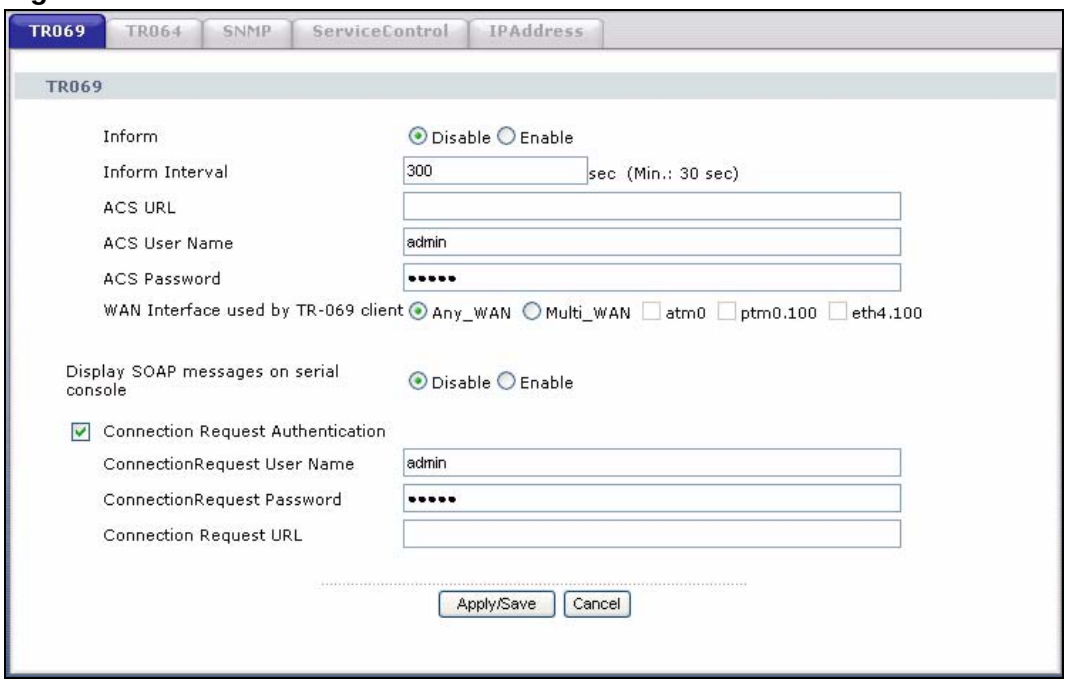
21.2 The TR-069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your P-2812HNU-51c, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the P-2812HNU-51c, modify settings, perform firmware upgrades as well as monitor and diagnose the P-2812HNU-51c. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Advanced > Remote MGMT** to open the following screen. Use this screen to configure your P-2812HNU-51c to be managed by an ACS.

Figure 167 TR-069



The following table describes the fields in this screen.

Table 112 TR-069

LABEL	DESCRIPTION
Inform	Select **Enable** to activate remote management via TR-069 on the WAN. Otherwise, select **Disable**.
Inform Interval	Enter the time interval (in seconds) at which the P-2812HNU-51c sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes. If you select **Multi_WAN**, you should also select the pre-configured WAN connection(s).
Display SOAP messages on serial console	Select **Enable** to show the SOAP messages on the console.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.

Table 112 TR-069 (continued)

LABEL	DESCRIPTION
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the P-2812HNU-51c, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the P-2812HNU-51c, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the P-2812HNU-51c.
Apply/Save	Click this button to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21.3 The TR-064 Screen

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

Click **Advanced > Remote MGMT** > **TR064** to open the following screen.

Figure 168 TR-064

The following table describes the fields in this screen.

Table 113 TR-064

LABEL	DESCRIPTION
Enanble TR064	Select the check box to activate management via TR-064 on the LAN.
Apply	Click this button to save your changes back to the P-2812HNU-51c.

21.4 The SNMP Screen

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. Your P-2812HNU-51c supports SNMP agent functionality, which allows a manager station to manage and monitor the P-2812HNU-51c through the network.

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the P-2812HNU-51c). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

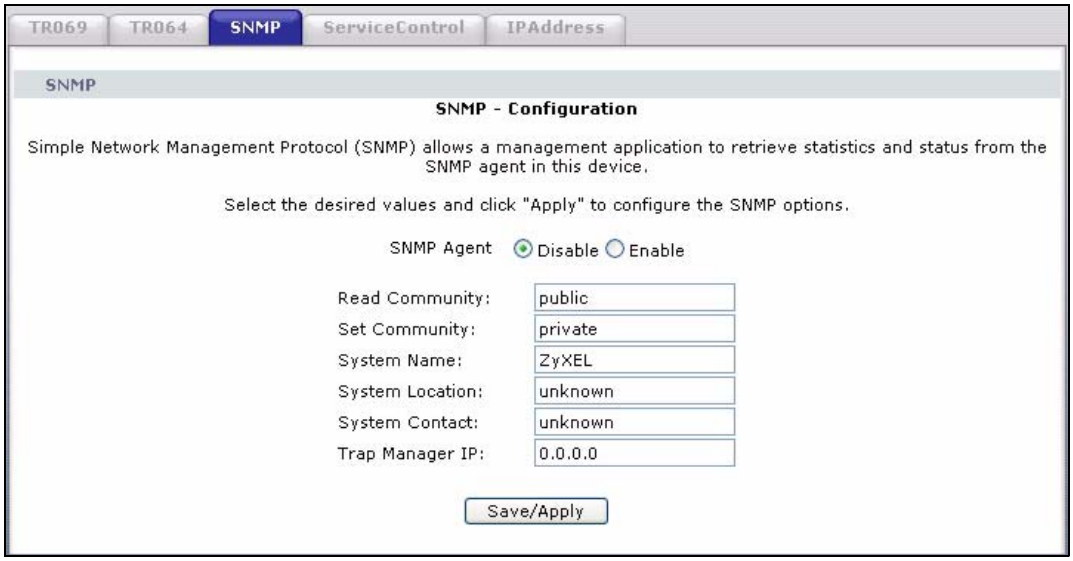
SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 114 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

Click **Advanced > Remote MGMT > SNMP** to open the following screen. Use this screen to configure the P-2812HNU-51c SNMP settings.

Figure 169 SNMP



The following table describes the fields in this screen.

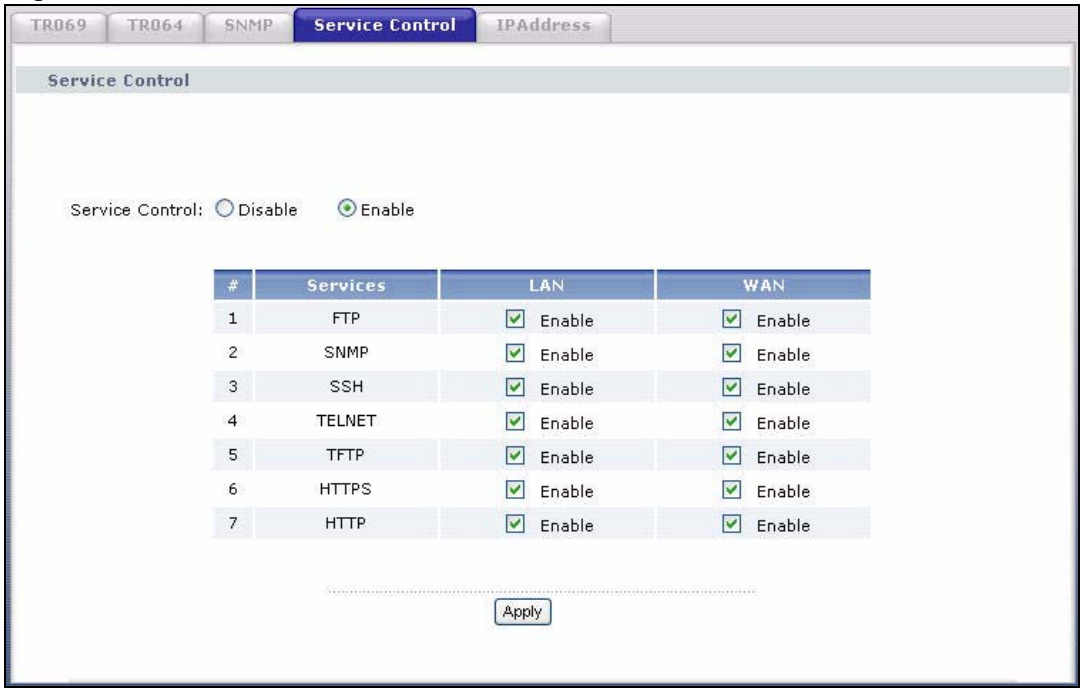
Table 115 SNMP

LABEL	DESCRIPTION
SNMP Agent	Select **Enable** to allow a manager station to manage and monitor the P-2812HNU-51c through the network via SNMP. Otherwise, select **Disable**.
Read Community	Enter the **Read Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
System Name	Enter the system name of the P-2812HNU-51c.
System Location	Specify the geographic location of the P-2812HNU-51c.
System Contact	Enter the name of the person in charge of the P-2812HNU-51c.
Trap Manager IP	Type the IP address of the station to send your SNMP traps to.
Save/Apply	Click this button to save your changes back to the P-2812HNU-51c.

21.5 The Service Control Screen

Click **Advanced > Remote MGMT > Service Control** to open the following screen. Use this screen to decide what services you may use to access which P-2812HNU-51c interface.

Figure 170 Service Control



The following table describes the fields in this screen.

Table 116 Service Control

LABEL	DESCRIPTION
Service Control	Select **Enable** to turn on service control. Otherwise, select **Disable**.
#	This is the index number of the entry.
Services	This is the service you may use to access the P-2812HNU-51c.
LAN	Select the **Enable** check box for the corresponding services that you want to allow access to the P-2812HNU-51c from the LAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the P-2812HNU-51c from the WAN.
Apply	Click this button to save your changes back to the P-2812HNU-51c.

21.6 The IP Address Screen

Click **Advanced > Remote MGMT > IP Address** to open the following screen. Use this screen to specify the “trusted” computers from which an administrator may use a service to manage the P-2812HNU-51c.

Figure 171 IP Address

TR069
TR064
SNMP
ServiceControl
IPAddress
Access Control -- IP Address
The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List
Access Control Mode:
Disable
Enable
IP Address
Remove
192.168.1.99
Add
Remove

The following table describes the fields in this screen.

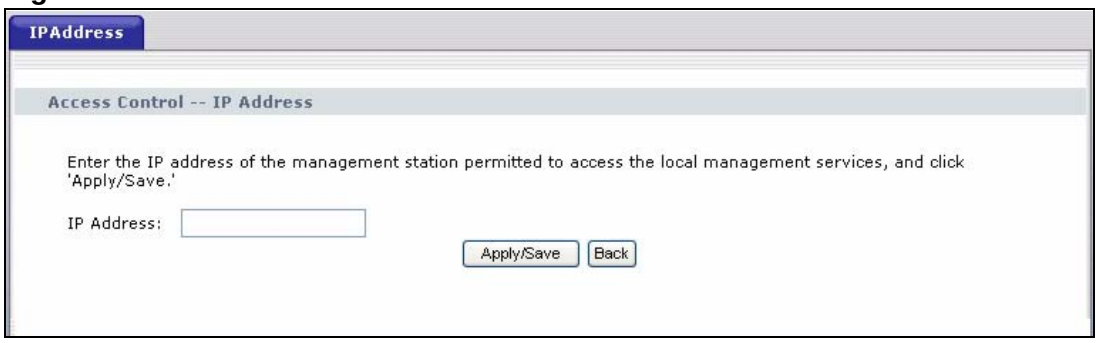
Table 117 IP Address

LABEL	DESCRIPTION
Access Control Mode	Select **Enable** to activate the secured client list. Select **Disable** to disable the list without deleting it.
IP Address	This is the IP address of the trusted computer from which you can manage the P-2812HNU-51c.
Remove	Select this check box and click the **Remove** button to delete this entry from the P-2812HNU-51c.
Add	Click this button to create a new entry.
Remove	Click this button to delete the selected entry.

21.6.1 Adding an IP Address

Click the **Add** button in the **IP Address** screen to open the following screen.

Figure 172 IP Address: Add


IPAddress
Access Control -- IP Address
Enter the IP address of the management station permitted to access the local management services, and click 'Apply/Save.'
IP Address:
Apply/Save
Back

The following table describes the fields in this screen.

Table 118 IP Address: Add

LABEL	DESCRIPTION
IP Address	Enter the IP address of the trusted computer from which you can manage the P-2812HNU-51c.
Apply/Save	Click this button to save your changes back to the P-2812HNU-51c.
Back	Click this button to return to the previous screen without saving.

22

Universal Plug-and-Play (UPnP)

22.1 Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

22.1.1 What You Can Do in this Chapter

The **UPnP** screen lets you enable UPnP on the P-2812HNU-51c (Section 22.3 on page 340).

22.2 What You Need to Know

Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the P-2812HNU-51c allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

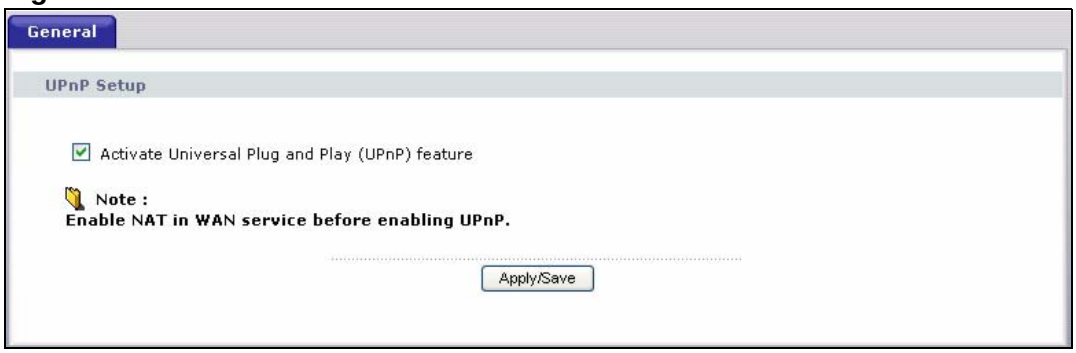
See the following sections for examples of installing and using UPnP.

22.3 The UPnP Screen

Click **Advanced > UPnP** to display the screen shown next.

See Section 22.1 on page 339 for more information.

Figure 173 Advanced > UPnP



The following table describes the fields in this screen.

Table 119 Advanced > UPnP

LABEL	DESCRIPTION
Activate Universal Plug and Play (UPnP) Feature	Select this check box to enable UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the P-2812HNU-51c's IP address (although you must still enter the password to access the web configurator).
Apply/Save	Click this to save the setting to the P-2812HNU-51c.

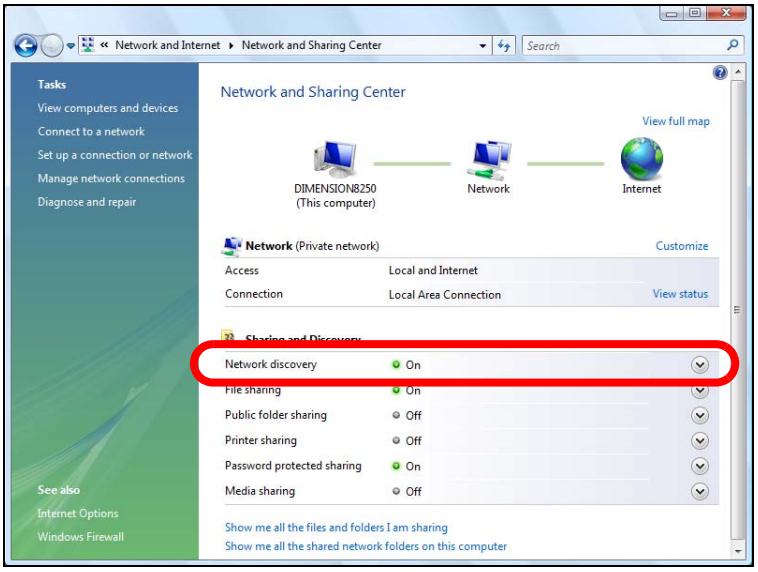
22.4 Installing UPnP in Windows

This section shows you how to configure or install UPnP in Windows.

22.4.1 Windows 7

Windows 7 already has UPnP installed. To enable it:

1. Click **Start > Control Panel** and select **Network and Internet**.
2. Click **Network and Sharing Center**.
3. In the **Network and Sharing** window, set **Network Discovery** to **On**. This activates the UPnP feature in Windows 7



22.4.2 Windows XP

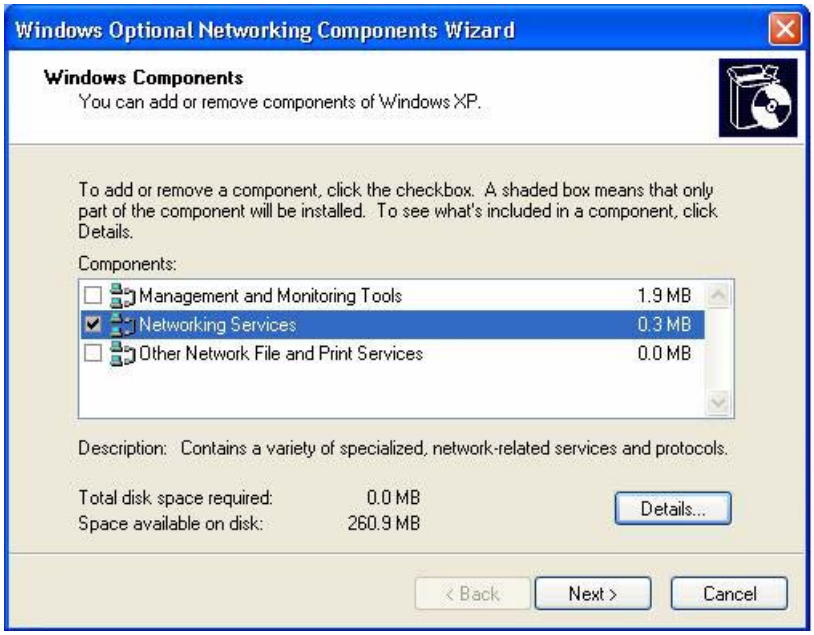
To install the UPnP in Windows XP:

1 Click **Start** and **Control Panel**.

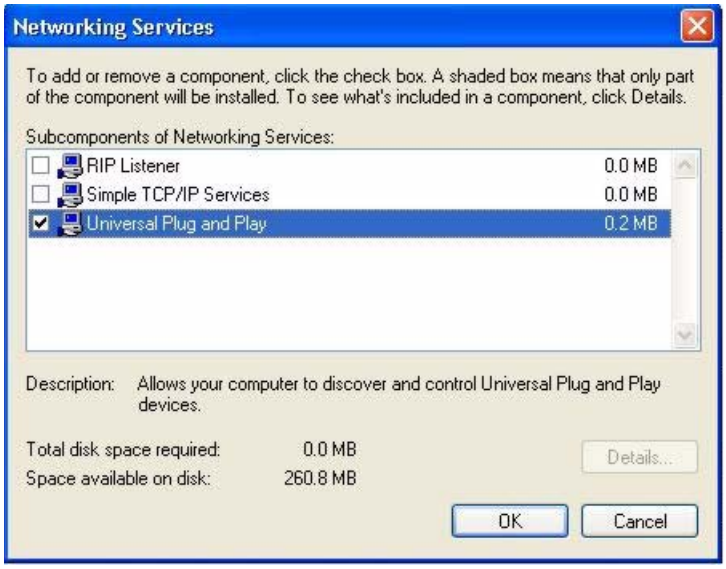
2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

22.5 Using UPnP in Windows XP

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the P-2812HNU-51c.

Make sure the computer is connected to a LAN port of the P-2812HNU-51c. Turn on your computer and the P-2812HNU-51c.

22.5.1 Auto-discover Your UPnP-enabled Network Device

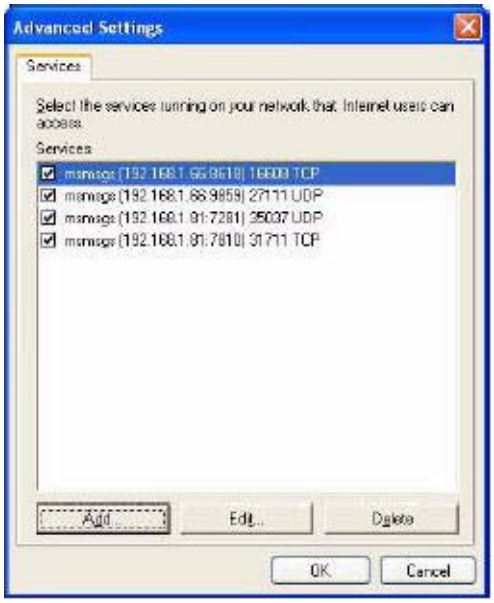
1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

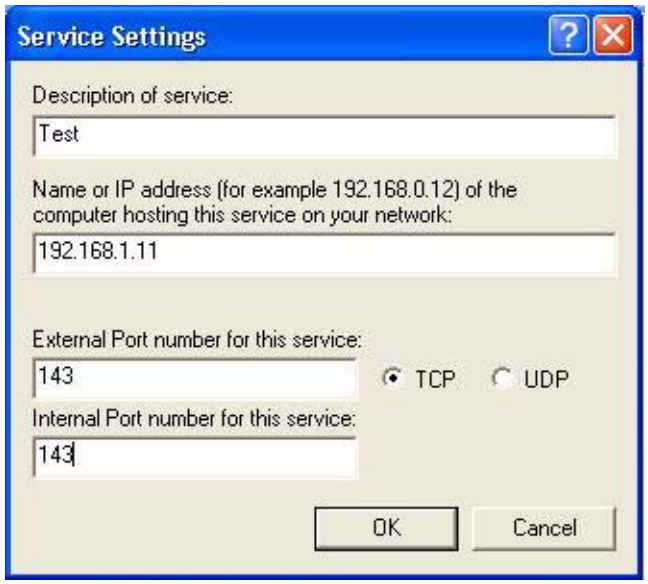
2 Right-click the icon and select **Properties**.

3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.





5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

7 Double-click on the icon to display your current Internet connection status.

22.5.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the P-2812HNU-51c without finding out the IP address of the P-2812HNU-51c first. This comes helpful if you do not know the IP address of the P-2812HNU-51c.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your P-2812HNU-51c and select **Invoke**. The web configurator login screen displays.

6 Right-click on the icon for your P-2812HNU-51c and select **Properties**. A properties window displays with basic information about the P-2812HNU-51c.

23

Parental Control

23.1 Overview

Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the P-2812HNU-51c performs parental control on a specific user.

23.1.1 What You Can Do in this Chapter

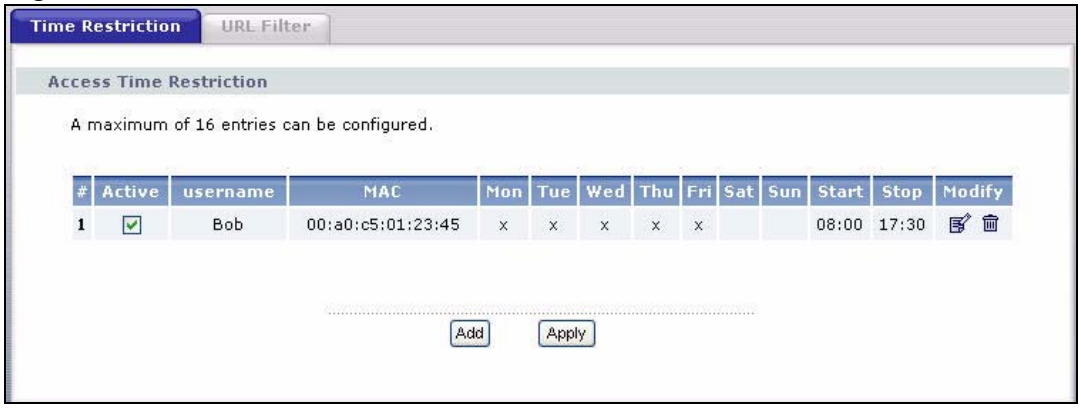
- The **Time Restriction** screen lets you give different time restrictions to each user of your network (Section 23.2 on page 349).
- The **URL Filter** screen lets you restrict home network users from viewing inappropriate websites (Section 23.3 on page 351).

23.2 The Time Restriction Screen

Use this screen to view the schedules and enable parental control on a specific user during certain periods.

Click **Advanced Setup > Parental Control** to open the following screen.

Figure 174 Parental Control > Time restriction


Time Restriction
URL Filter
Access Time Restriction
A maximum of 16 entries can be configured.
Active username MAC Mon Tue Wed Thu Fri Sat Sun Start Stop Modify
1 Bob 00:a0:c5:01:23:45 x x x x x 08:00 17:30
Add
Apply

The following table describes the fields in this screen.

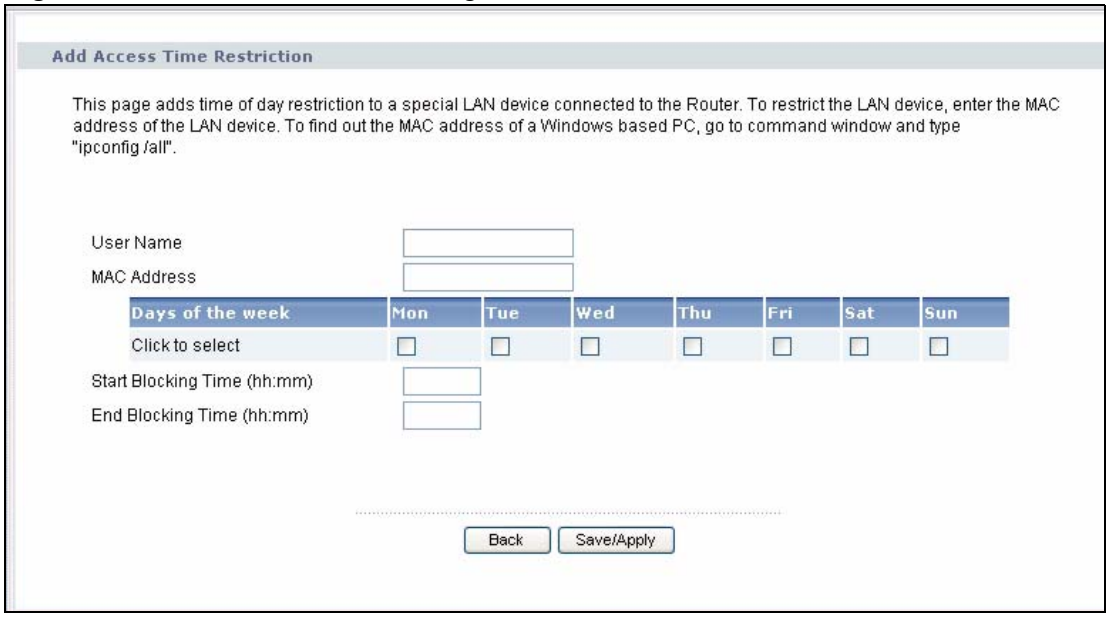
Table 120 Parental Control > Time Restriction

LABEL	DESCRIPTION
#	This shows the index number of the schedule.
Active	Select the check box to enable the schedule.
username	This shows the name of the user.
MAC	This shows the MAC address of the LAN user's computer to which this schedule applies.
Mon ~ Sun	**x** indicates the day(s) on which parental control is enabled.
Start	This shows the time when the schedule starts.
Stop	This shows the time when the schedule ends.
Modify	Click the **Edit** icon to go to the screen where you can edit the schedule. Click the **Remove** icon to delete an existing schedule.
Add	Click **Add** to create a new schedule.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.

23.2.1 Adding a Schedule

Click the **Add** button in the **Time Restriction** screen to open the following screen. Use this screen to configure a restricted access schedule for a specific user on your network.

Figure 175 Time Restriction Configuration


Add Access Time Restriction
This page adds time of day restriction to a special LAN device connected to the Router. To restrict the LAN device, enter the MAC address of the LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".
User Name
MAC Address
Days of the week
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Click to select
Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)
Back
Save/Apply

The following table describes the fields in this screen.

Table 121 Time Restriction Configuration

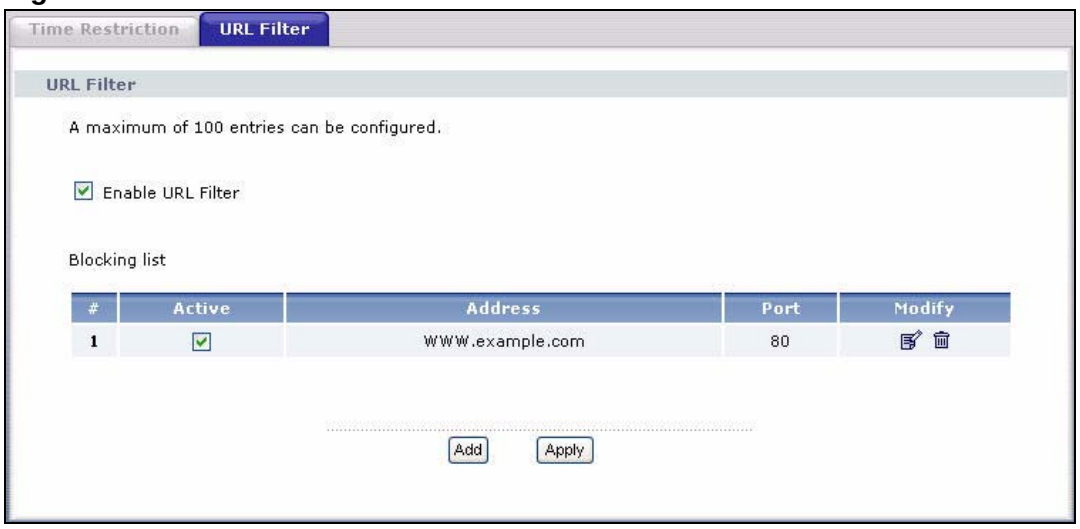
LABEL	DESCRIPTION
User Name	Enter the name of the user.
MAC Address	Enter the MAC address of the LAN user's computer to which this schedule applies.
Days of the week	Select check boxes for the days that you want the P-2812HNU-51c to perform parental control.
Start Blocking Time End Blocking Time	Enter the time period of each day, in 24-hour format, during which parental control will be enforced.
Back	Click this button to return to the previous screen without saving any changes.
Save/Apply	Click this button to save your settings back to the P-2812HNU-51c.

23.3 The URL Filter Screen

Use this screen to configure URL filtering settings to block the users on your network from accessing certian web sites.

Click **Advanced Setup > Parental Control > URL Filter** to open the following screen.

Figure 176 Parental Control > URL Filter



The following table describes the fields in this screen.

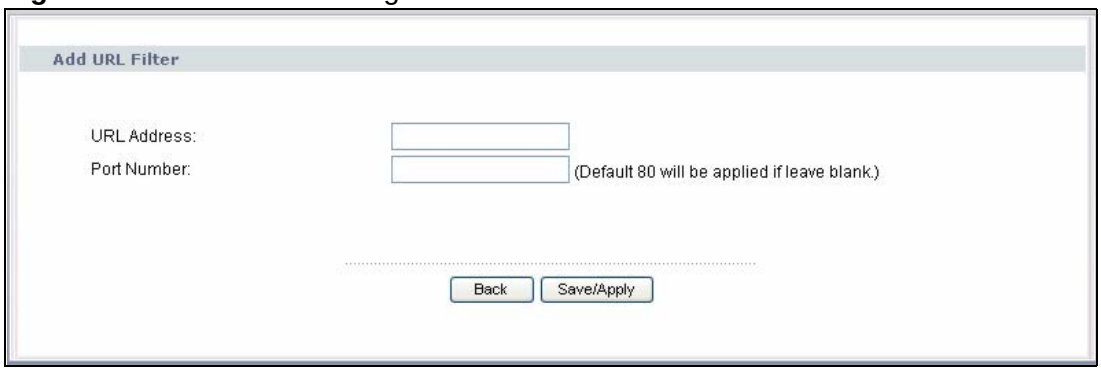
Table 122 Parental Control > URL Filter

LABEL	DESCRIPTION
Enable URL Filter	Select the check box to enable URL filtering on the P-2812HNU-51c.
Blocking list	The P-2812HNU-51c prohibits the users from viewing the Web sites with the URLs listed below.
#	This is the index number of the rule.
Active	Select the check box to enable the filtering rule.
Address	This is the URL of the web site in this rule.
Port	This is the port number the web server uses to forward HTTP traffic.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Remove** icon to delete an existing rule.
Add	Click **Add** to create a new rule.
Apply	Click this button to save your settings back to the P-2812HNU-51c.

23.3.1 Adding URL Filter

Click the **Add** button in the **URL Filter** screen to open the following screen.

Figure 177 URL Filter Configuration



The following table describes the fields in this screen.

Table 123 URL Filter Configuration

LABEL	DESCRIPTION
URL Address	Enter the URL of web site to which the P-2812HNU-51c blocks or allows access.
Port Number	Specify the port number the web server uses to forward HTTP traffic.
Back	Click this button to return to the previous screen without saving any changes.
Save/Apply	Click this button to save your settings back to the P-2812HNU-51c.

24

Interface Group

24.1 Overview

By default, all LAN and WAN interfaces on the P-2812HNU-51c are in the same group and can communicate with each other. You can create multiple groups to have the P-2812HNU-51c assign the IP addresses in different domains to different groups. Each group acts as an independent network on the P-2812HNU-51c.

24.1.1 What You Can Do in this Chapter

The **Interface Group** screen lets you create multiple networks on the P-2812HNU-51c (Section 24.2 on page 353).

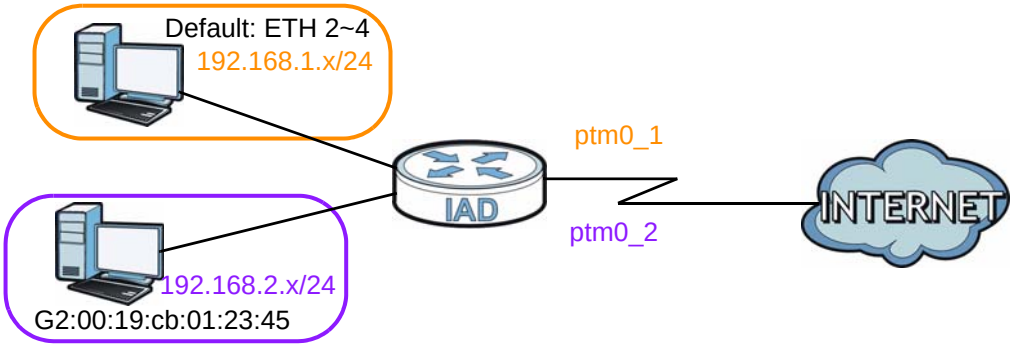
24.2 The Interface Group Screen

You can manually add a LAN interface to a new group. Alternatively, you can have the P-2812HNU-51c automatically add the incoming traffic and the LAN interface on which traffic is received to the new group when its source MAC address or DHCP option information matches the predefined filtering criteria.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the P-2812HNU-51c assigns to the clients in the default and/or user-defined groups. If you set the P-2812HNU-51c to assign IP addresses based on the client's source MAC address or DHCP option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See Chapter 6 on page 137 for more information.

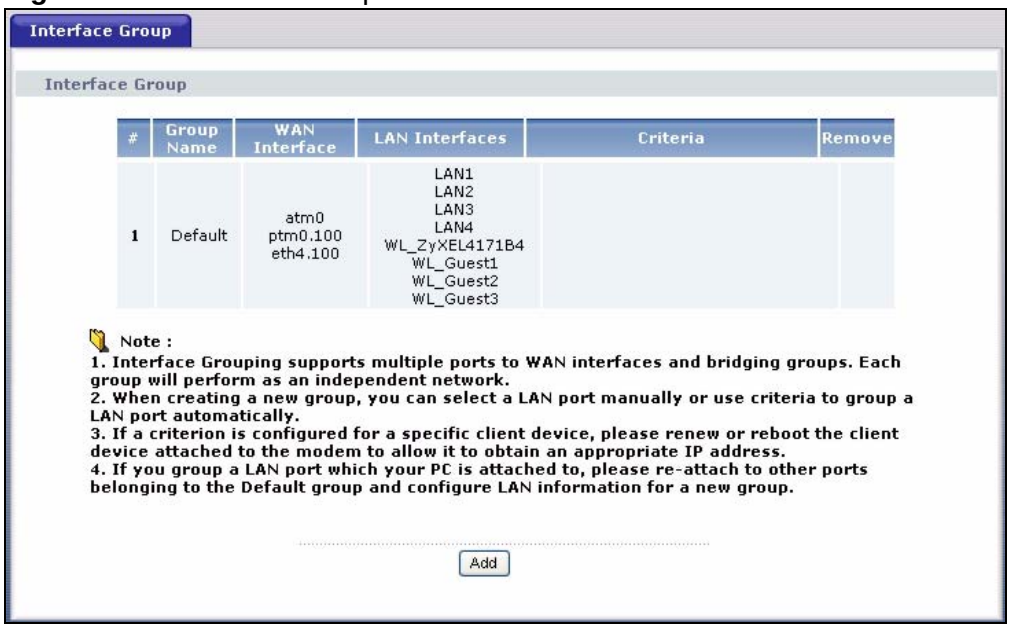
In the following example, the client that sends packets with the source MAC address 00:19:cb:01:23:45 is assigned the IP address 192.168.2.2 and uses the WAN interface ptm0_2.

Figure 178 Interface Grouping Application



Click **Advanced Setup > Interface Group** to open the following screen.

Figure 179 Interface Group


Interface Group
Interface Group
Group Name WAN Interface LAN Interfaces Criteria Remove
1 Default atm0 ptm0.100 eth4.100 LAN1 LAN2 LAN3 LAN4 WL_ZyXEL4171B4 WL_Guest1 WL_Guest2 WL_Guest3
Note :
1. Interface Grouping supports multiple ports to WAN interfaces and bridging groups. Each group will perform as an independent network.
2. When creating a new group, you can select a LAN port manually or use criteria to group a LAN port automatically.
3. If a criterion is configured for a specific client device, please renew or reboot the client device attached to the modem to allow it to obtain an appropriate IP address.
4. If you group a LAN port which your PC is attached to, please re-attach to other ports belonging to the Default group and configure LAN information for a new group.
Add

The following table describes the fields in this screen.

Table 124 Interface Grouping

LABEL	DESCRIPTION
#	This shows the index number of the entry.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering criteria for the goup.

Table 124 Interface Grouping (continued)

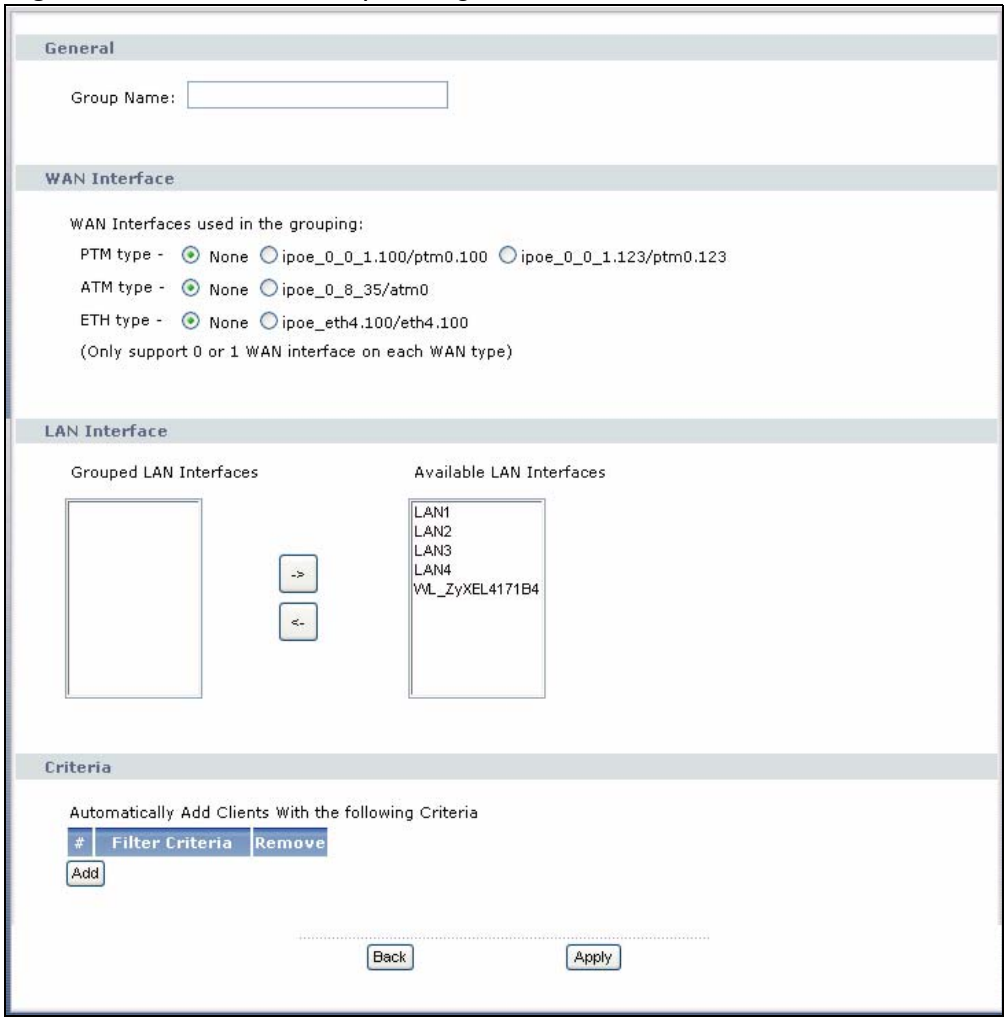
LABEL	DESCRIPTION
Remove	Click the **Remove** icon to delete the group.
Add	Click this button to create a new group.

24.2.1 Interface Group Configuration

Click the **Add** button in the **Interface Group** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to a group only.

Figure 180 Interface Group Configuration



The following table describes the fields in this screen.

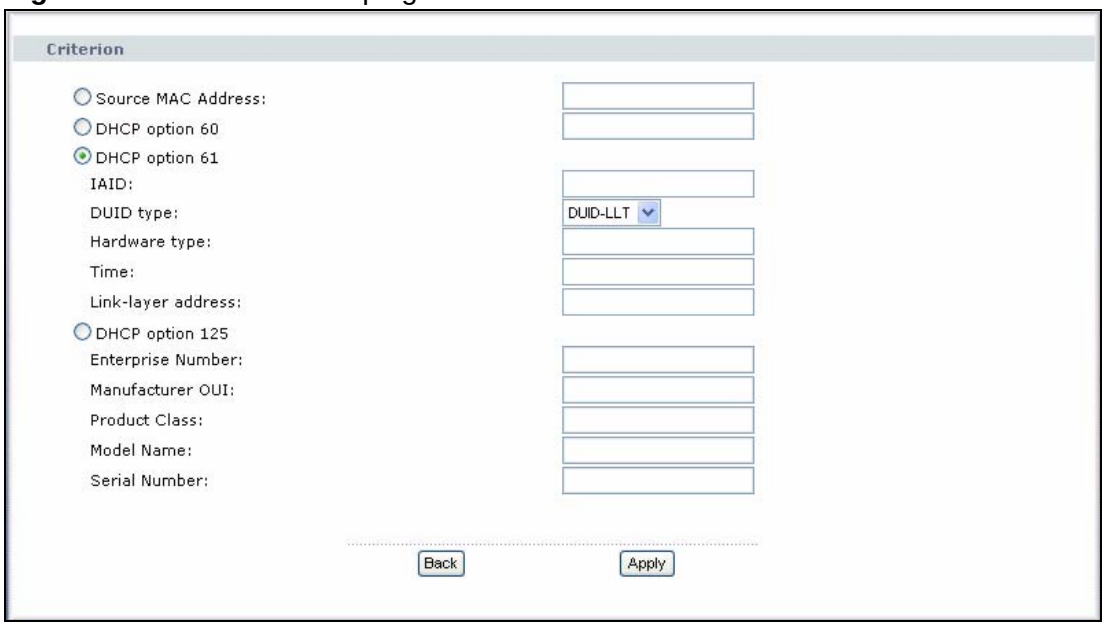
Table 125 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group.
WAN Interfaces used in the grouping	Select a WAN interface to be used in this group. Select **None** to not add a WAN interface to this group.
Grouped LAN Interfaces Available LAN Interfaces	Select a LAN or wireless LAN interface in the **Available LAN Interfaces** and use the left-facing arrow to move it to the **Grouped LAN Interfaces** to add the interface to this group. To remove a LAN or wireless LAN interface from the **Grouped LAN Interfaces**, use the righ-facing arrow.
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
Remove	Click the **Remove** icon to delete this rule from the P-2812HNU-51c.
Add	Click this button to create a new rule.
Back	Click this button to return to the previous screen without saving any changes.
Apply	Click this button to save your settings back to the P-2812HNU-51c.

24.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen.

Figure 181 Interface Grouping Criteria



The following table describes the fields in this screen.

Table 126 Interface Grouping Criteria

LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID Type	Select **DUID-LLT** (DUID Based on Link-layer Address Plus Time) to enter the hardware type, a time value and the MAC address of the device. Select **DUID-EN** (DUID Assigned by Vendor Based upon Enterprise Number) to enter the vendor's registered enterprise number. Select **DUID-LL** (DUID Based on Link-layer Address) to enter the device's hardware type and hardware address (MAC address) in the following fields. Select **Other** to enter any string that identifies the device in the **DUID** field.
Hardware type	Enter the 16-bit hardware type of the device from which the traffic comes. For example, Ethernet is 1 and Experimental Ethernet is 2.
Time	Enter the time (in seconds since midnight (UTC), January 1, 2000) the DUID is generated.
Link-layer address	Enter the MAC address of the device.
Enterprise number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Identifier	Enter a unique identifier assigned by the vendor.
DUID	Enter the DHCP Unique Identifier (DUID) of the device.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Product Class	Enter the product class of the device.
Model Name	Enter the model name of the device.
Serial Number	Enter the serial number of the device.
Back	Click this button to return to the previous screen without saving any changes.
Apply	Click this button to save your settings back to the P-2812HNU-51c.

25

E-mail Notification

25.1 Overview

A mail server is an application or a computer that runs such an application to receive, forward and deliver e-mail messages.

To have the P-2812HNU-51c send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

25.1.1 What You Can Do in this Chapter

The **Email Notification** screens let you configure up to two mail servers and sender addresses on the P-2812HNU-51c (Section 25.2 on page 359).

25.2 The Email Notification Screen

Click **Advanced > Email Notification** to open the **Email Notification** screen. Use this screen to view, remove and add mail server information on the P-2812HNU-51c.

Figure 182 Advanced > Email Notification

The following table describes the labels in this screen.

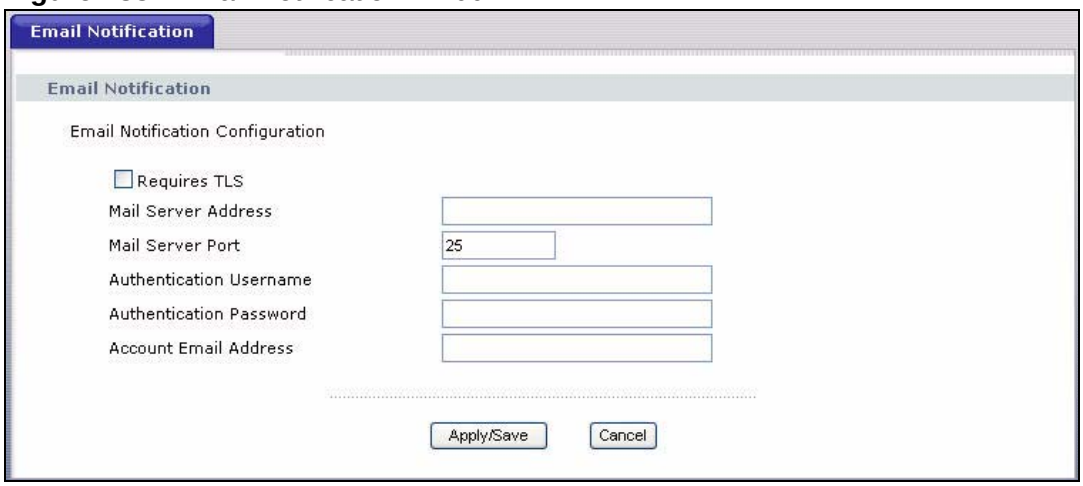
Table 127 Advanced > Email Notification

LABEL	DESCRIPTION
Mail Server Address	This field displays the server name or the IP address of the mail server.
Mail Server Port	This field displays the number of the port used for mail transport on the mail server.
Username	This field displays the user name of the sender's mail account.
Password	This field displays the password of the sender's mail account.
Email Address	This field displays the e-mail address that you want to be in the from/ sender line of the e-mail that the P-2812HNU-51c sends.
Requires TLS	This field displays whether SSL/TLS authentication is required for the mail server.
Remove	Select the check box of the entry you want to delete and click the **Remove** button.
Add	Click this button to create a new entry. This button is not available if you have configured two entries.
Remove	Click this button to delete the selected entry(ies).

25.2.1 Email Notification Edit

Click the **Add** button in the **Email Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

Figure 183 Email Notification > Add



The following table describes the labels in this screen.

Table 128 Email Notification > Add

LABEL	DESCRIPTION
Requires TLS	Select this option to enable SSL/TLS authentication. If mail server authentication is needed but this feature is disabled, you will not receive e-mail. Secure Socket Layer (SSL) and Transport Layer Security (TLS) are application-level protocols that enable secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the **Account Email Address** field. If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Mail Server Port	Enter the number of the port the mail server uses for mail transport.
Authentication Username	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the **Account Email Address** field.
Authentication Password	Enter the password associated with the user name above.
Account Email Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the P-2812HNU-51c sends. If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.
Apply/Save	Click this button to save your changes and return to the previous screen.
Cancel	Click this button to begin configuring this screen afresh.

26

System Settings

26.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

26.1.1 What You Can Do in this Chapter

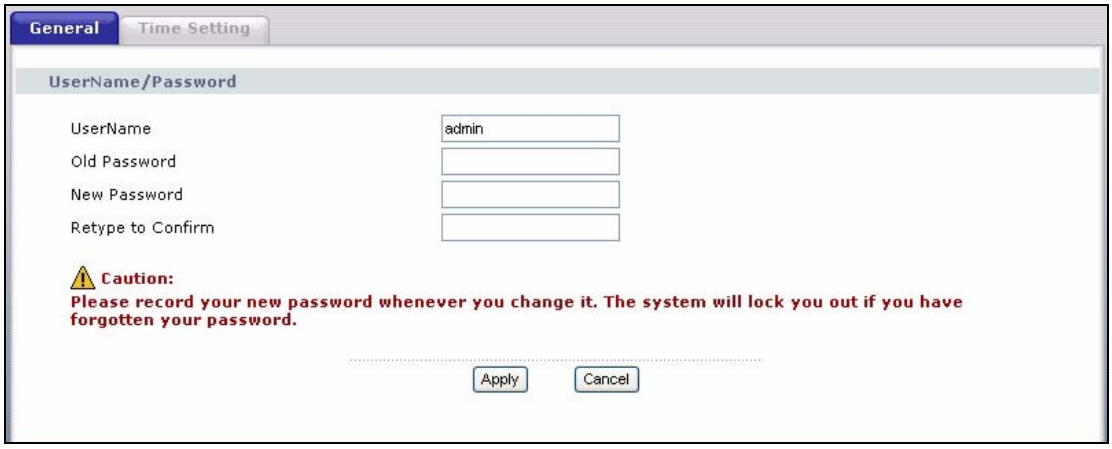
- The **General** screen lets you configure system settings (Section 26.2 on page 363).
- The **Time Setting** screen lets you set the system time (Section 26.3 on page 364).

26.2 The General Screen

Use the **General** screen to configure system settings such as the system password.

Click **Maintenance > System** to open the **General** screen.

Figure 184 Maintenance > System > General



The following table describes the labels in this screen.

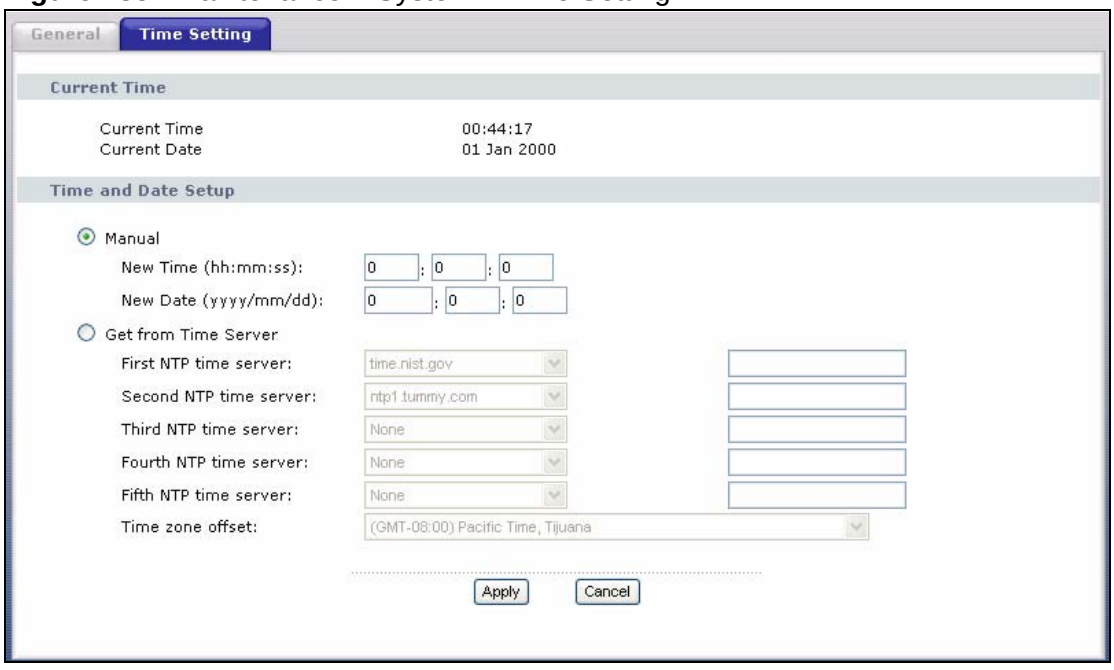
Table 129 Maintenance > System > Genera

LABEL	DESCRIPTION
UserName	Type the user name you use to access the system.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the P-2812HNU-51c.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

26.3 The Time Setting Screen

To change your P-2812HNU-51c's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the P-2812HNU-51c's time based on your local time zone.

Figure 185 Maintenance > System > Time Setting



The following table describes the fields in this screen.

Table 130 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time	
Current Time	This field displays the time of your P-2812HNU-51c. Each time you reload this page, the P-2812HNU-51c synchronizes the time with the time server.
Current Date	This field displays the date of your P-2812HNU-51c. Each time you reload this page, the P-2812HNU-51c synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this option to enter the time and date manually.
Get from Time Server	Select this option to have the P-2812HNU-51c get the time and date from the time server you specified below.
First NTP time server Second NTP time server Third NTP time server Fourth NTP time server Fifth NTP time server	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Select **None** if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time zone offset	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Apply	Click **Apply** to save your changes back to the P-2812HNU-51c.
Cancel	Click **Cancel** to begin configuring this screen afresh.

27 Logs

27.1 Overview

This chapter contains information about configuring general log settings and viewing the P-2812HNU-51c's logs.

The web configurator allows you to choose which categories of events and/or alerts to have the P-2812HNU-51c log and then display the logs or have the P-2812HNU-51c send them to a syslog server.

27.1.1 What You Can Do in this Chapter

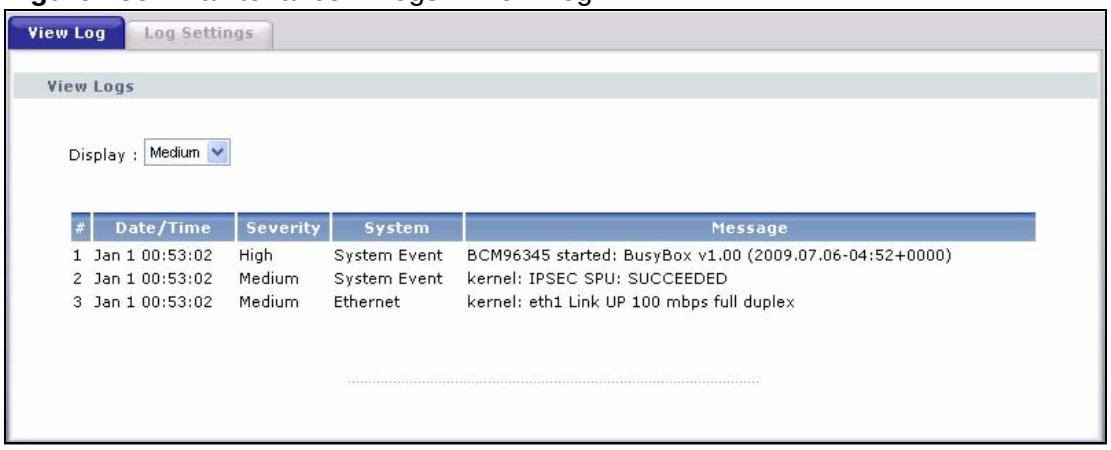
- The **View Log** screen lets you see the logs for the categories that you selected in the **Log Settings** screen (Section 27.2 on page 367).
- The **Log Settings** screen lets you configure to where the P-2812HNU-51c is to send logs and which logs and/or immediate alerts the P-2812HNU-51c is to record (Section 27.3 on page 368).

27.2 The View Log Screen

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 27.3 on page 368).

The log wraps around and deletes the old entries after it fills.

Figure 186 Maintenance > Logs > View Log


View Log
Log Settings
View Logs
Display : Medium
Date/Time Severity System Message
1 Jan 1 00:53:02 High System Event BCM96345 started: BusyBox v1.00 (2009.07.06-04:52+0000)
2 Jan 1 00:53:02 Medium System Event kernel: IPSEC SPU: SUCCEEDED
3 Jan 1 00:53:02 Medium Ethernet kernel: eth1 Link UP 100 mbps full duplex

The following table describes the fields in this screen.

Table 131 Maintenance > Logs > View Log

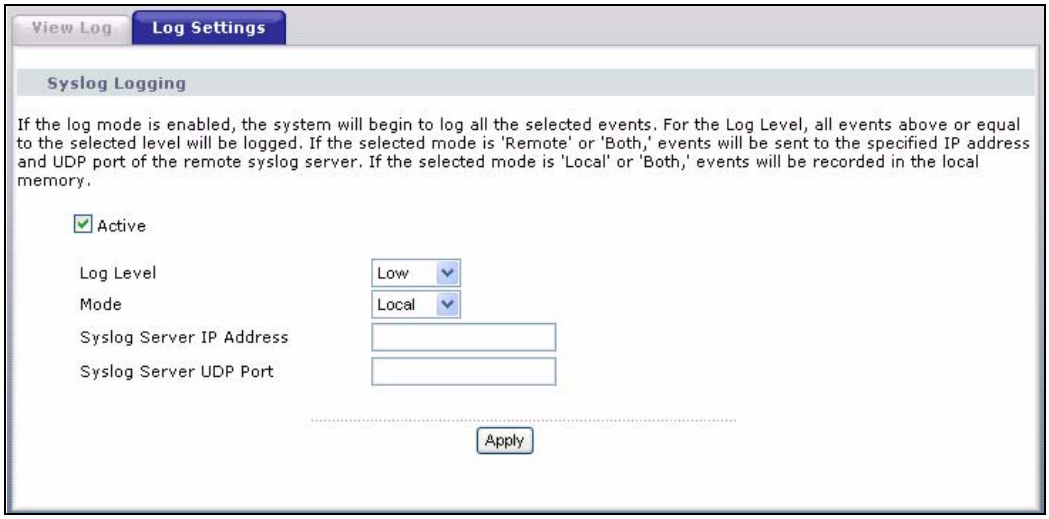
LABEL	DESCRIPTION
Display	Select a severity level of logs to view. The P-2812HNU-51c displays the logs with the severity level equal to or higher than what you selected.
#	This field is a sequential value and is not associated with a specific entry.
Date/Time	This field displays the time the log was recorded.
Severity	This field displays the severity level of the log.
System	This field displays the system module from which the logs come.
Message	This field states the reason for the log.

27.3 The Log Settings Screen

Use the **Log Settings** screen to configure to where the P-2812HNU-51c is to send logs and which logs and/or immediate alerts the P-2812HNU-51c is to record and display.

To change your P-2812HNU-51c's log settings, click **Maintenance > Logs** > **Log Settings**. The screen appears as shown.

Figure 187 Maintenance > Logs > Log Settings


View Log
Log Settings
Syslog Logging
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Active
Log Level
Low
Mode
Local
Syslog Server IP Address
Syslog Server UDP Port
Apply

The following table describes the fields in this screen.

Table 132 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Active	Select to enable or disable system logging.
Log Level	Select the severity level of the logs that you want the P-2812HNU-51c to display, record and send to the log server. The P-2812HNU-51c displays and records the logs with the severity level equal to or higher than what you selected.
Mode	Select **Local** to record the logs and store them in the local memory of the P-2812HNU-51c only. Select **Remote** to send logs to the specified log server. Select **Both** to record the logs and store them in the local memory and also send logs to the log server.
Syslog Server IP Address	Enter the server name or the IP address of the log server.
Syslog Server UDP Port	Enter the UDP port of the log server.
Apply	Click **Apply** to save your customized settings.

28 Tools

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your P-2812HNU-51c.

28.1 Overview

This chapter explains how to upload new firmware, manage configuration files and restart your P-2812HNU-51c.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your P-2812HNU-51c.

28.1.1 What You Can Do in this Chapter

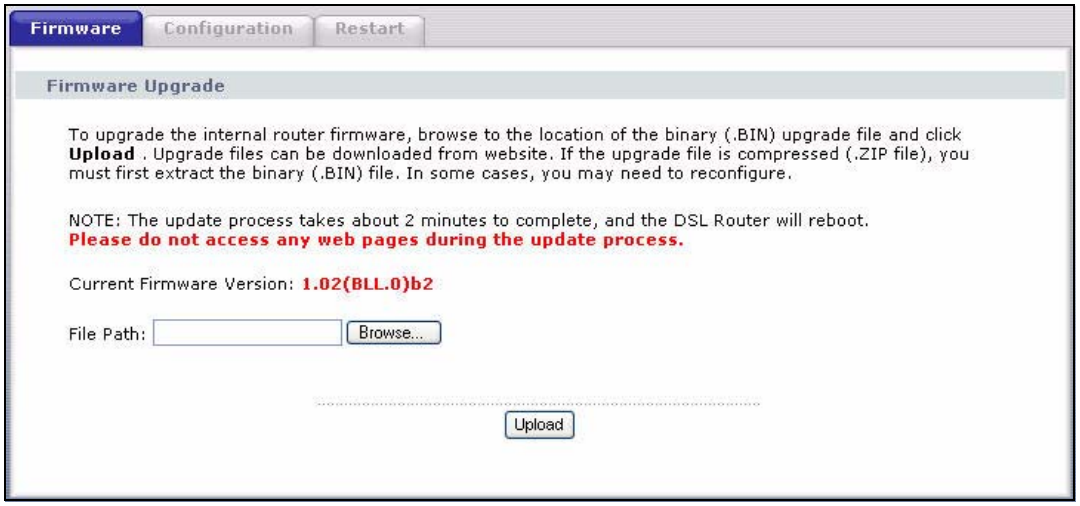
- The **Firmware** screen lets you upload firmware to your device (Section 28.2 on page 372).
- The **Configuration** screen lets you backup and restore device configurations (Section 28.3 on page 374). You can also reset your device settings back to the factory default.
- The **Restart** screen lets you restart your P-2812HNU-51c (Section 28.4 on page 376).

28.2 The Firmware Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your P-2812HNU-51c. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the P-2812HNU-51c while firmware upload is in progress!

Figure 188 Maintenance > Tools > Firmware


Firmware
Configuration
Restart
Firmware Upgrade
To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload . Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.
NOTE: The update process takes about 2 minutes to complete, and the DSL Router will reboot.
Please do not access any web pages during the update process.
Current Firmware Version: 1.02(BLL.0)b2
File Path:
Browse...
Upload

The following table describes the labels in this screen.

Table 133 Maintenance > Tools > Firmware

LABEL	DESCRIPTION
Current Firmware Version	This is the present firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the P-2812HNU-51c again.

Figure 189 Firmware Upload In Progress

DSL Router Update
Please Wait ...
Uploading is in progress. The DSL Router will reboot upon completion. This process will take about 2 minutes.

The P-2812HNU-51c automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 190 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **Status** screen.

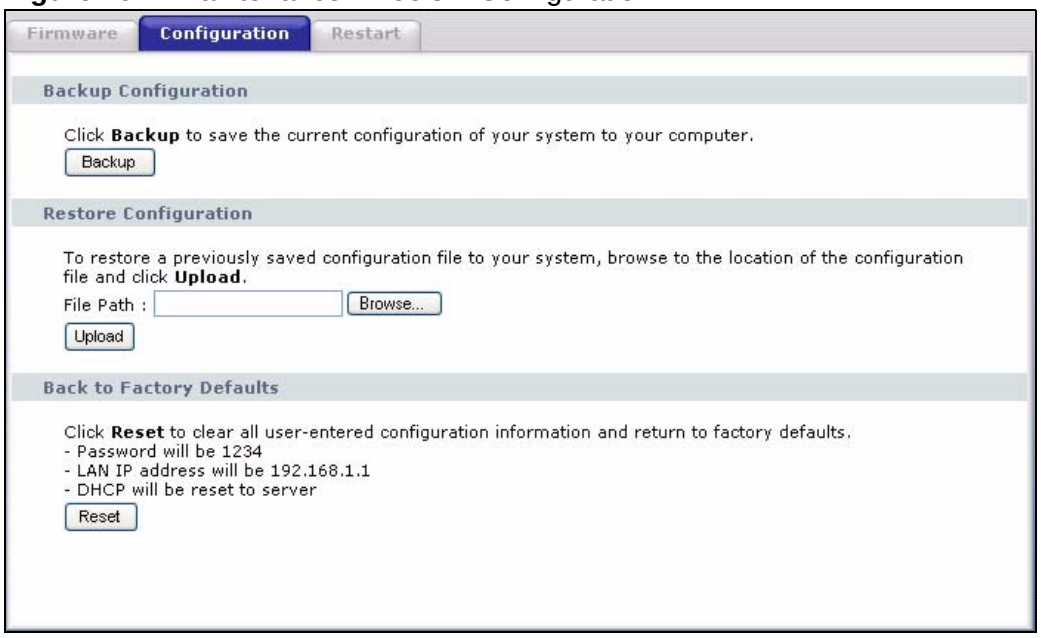
If the upload was not successful, the following screen will appear. Click **Tools** to go back to the **Firmware** screen.

Figure 191 Error Message

28.3 The Configuration Screen

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 192 Maintenance > Tools > Configuration


Firmware
Configuration
Restart
Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path :
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults.
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server
Reset

Backup Configuration

Backup Configuration allows you to back up (save) the P-2812HNU-51c's current configuration to a file on your computer. Once your P-2812HNU-51c is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the P-2812HNU-51c's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your P-2812HNU-51c.

Table 134 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Do not turn off the P-2812HNU-51c while configuration file upload is in progress.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the P-2812HNU-51c again.

Figure 193 Configuration Upload Successful

DSL Router Update
Please Wait ...
Uploading is in progress. The DSL Router will reboot upon completion. This process will take about 2 minutes.

The P-2812HNU-51c automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 194 Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix B on page 417 for details on how to set up your computer’s IP address.

If the upload was not successful, the following screen will appear. Click **Tools > Configuration** to go back to the **Configuration** screen.

Figure 195 Configuration Upload Error

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the P-2812HNU-51c to its factory defaults. The following warning screen appears.

Figure 196 Reset Warning Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your P-2812HNU-51c. Refer to Section 1.5 on page 29 for more information on the **RESET** button.

28.4 The Restart Screen

System restart allows you to reboot the P-2812HNU-51c without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the P-2812HNU-51c reboot. This does not affect the P-2812HNU-51c's configuration.

Figure 197 Maintenance > Tools >Restart

Firmware
Configuration
Restart
System Restart
Click Restart to have the device perform a software restart. The SYS LED blinks as the device restarts and then stays steady on if the restart is successful.
Wait a minute before logging into the device again.
Restart

29

Diagnostic

29.1 Overview

The **Diagnostic** screens display information to help you identify problems with the P-2812HNU-51c.

The route between a CO VDSL switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

29.1.1 What You Can Do in this Chapter

- The **General** screen lets you ping an IP address or trace the route packets take to a host (Section 29.3 on page 380).
- The **802.1ag** screen lets you perform CFM actions (Section 29.4 on page 381).
- The **OAM Ping Test** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC. (Section 29.4 on page 381)

29.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

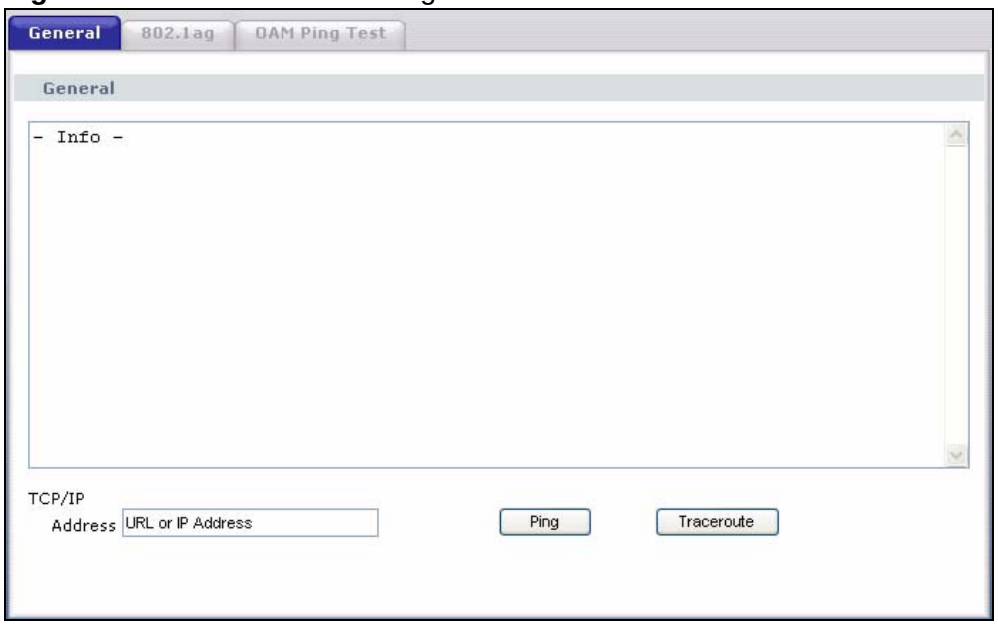
CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

29.3 The General Diagnostic Screen

Click **Maintenance > Diagnostic** to open the screen shown next. Ping and traceroute help check availability of remote hosts and also help troubleshoot network or Internet connections.

Figure 198 Maintenance > Diagnostic > General



The following table describes the fields in this screen.

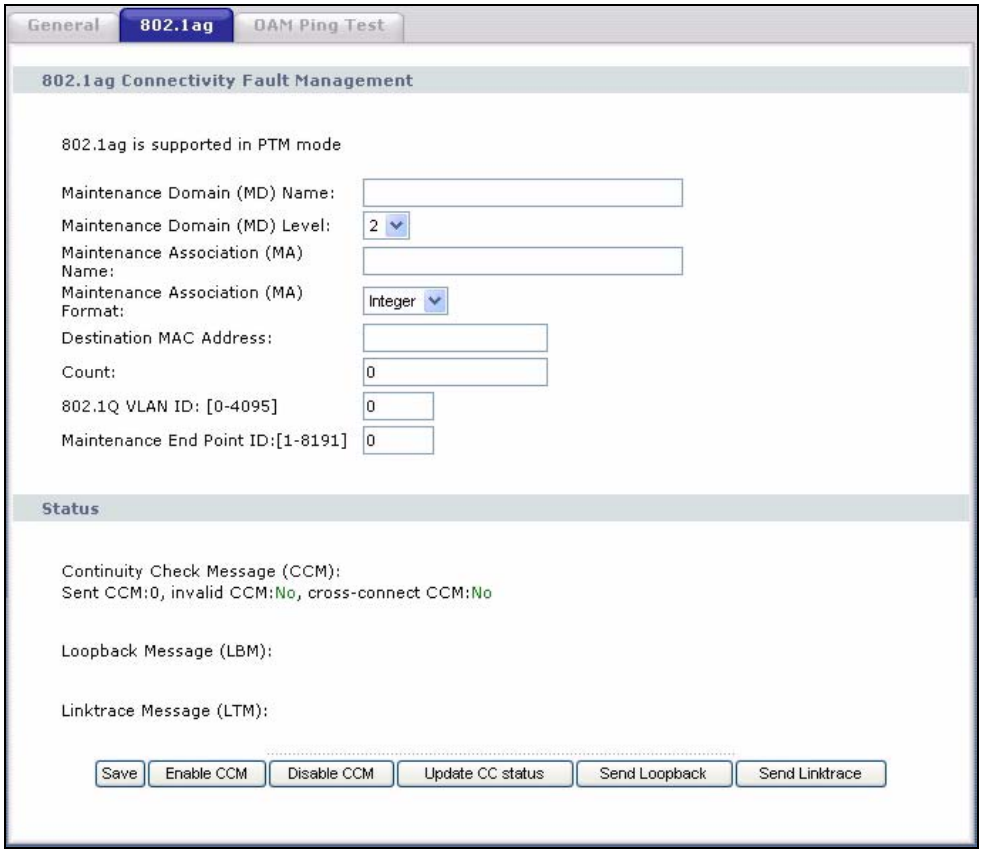
Table 135 Maintenance > Diagnostic > General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection or trace the route packets take to.
Ping	Click this button to ping the IP address that you entered.
Traceoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified host.

29.4 The 802.1ag Screen

Click **Diagnostic** to open the following screen. Use this screen to perform CFM actions.

Figure 199 802.1ag



The following table describes the fields in this screen.

Table 136 Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
Maintenance Domain (MD) Name	Type a name of up to 39 printable English keyboard characters for this MD. The combined length of the MD Name and MA name must be less or equal to 44bytes.
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.

Table 136 Maintenance > Diagnostic > 802.1ag (continued)

LABEL	DESCRIPTION
Maintenance Association (MA) Name	Type a name of up to 39 printable English keyboard characters for this MA. The combined length of the MD Name and MA name must be less or equal to 44bytes.
Maintenance Association (MA) Format	Select the format which the P-2812HNU-51c uses to send this MA information in the domain (MD). Options are **VID**, **String** and **Integer**. If you select **VID** or **Integer**, the P-2812HNU-51c adds the VLAN ID you specified for an MA in the CCM. If you select **String**, the P-2812HNU-51c adds the MA name you specified above in the CCM. Note: The MEPs in the same MA shoule use the same MA format.
Destination MAC Address	Enter the target device's MAC address to which the P-2812HNU-51c performs a CFM loopback test.
Count	Set how many times the P-2812HNU-51c send loopback messages (LBMs).
802.1Q VLAN ID	Type a VLAN ID (0-4095) for this MA.
Maintenance End Point ID	Enter an ID number (1-8191) for this MEP port. Each MEP port needs a unique ID number within an MD. The MEP ID is to identify an MEP port used when you perform a CFM action
Status	
Continuity Check Message (CCM)	This shows how many Connectivity Check Messages (CCMs) are sent and if there is any invalid CCM or cross-connect CCM.
Loopback Message (LBM)	This shows how many Loop Back Messages (LBMs) are sent and if there is any inorder or outorder Loop Back Response (LBR) received from a remote MEP.
Linktrace Message (LTM)	This shows the destination MAC address in the Link Trace Response (LTR).
Save	Click this to save your changes back to the P-2812HNU-51c.
Enable CCM	Click this button to have the selected MEP send Connectivity Check Messages (CCMs) to other MEPs.
Disable CCM	Click this button to disallow the selected MEP to send Connectivity Check Messages (CCMs) to other MEPs.
Update CC status	Click this button to reload the test result.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

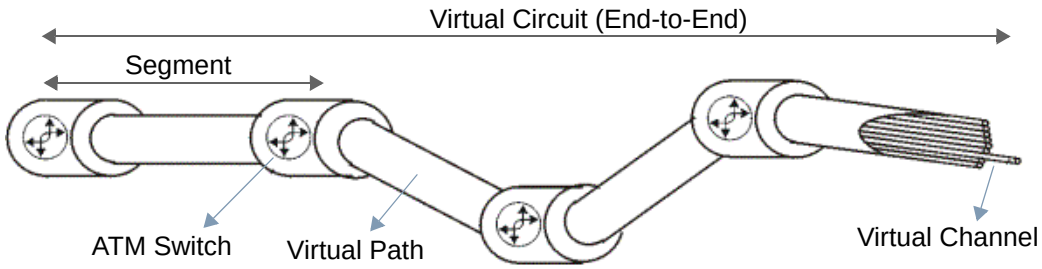
29.5 The OAM Ping Test Screen

Click **Maintenance > Diagnostic > OAM Ping Test** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a PVC. The P-2812HNU-51c sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the P-2812HNU-51c. The test result then displays in the text box.

ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel (VC) Logical connections between ATM devices
- Virtual Path (VP) A bundle of virtual channels
- Virtual Circuits A series of virtual paths between circuit end points

Figure 200 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path. A series of virtual paths make up a virtual circuit.

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefinded Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

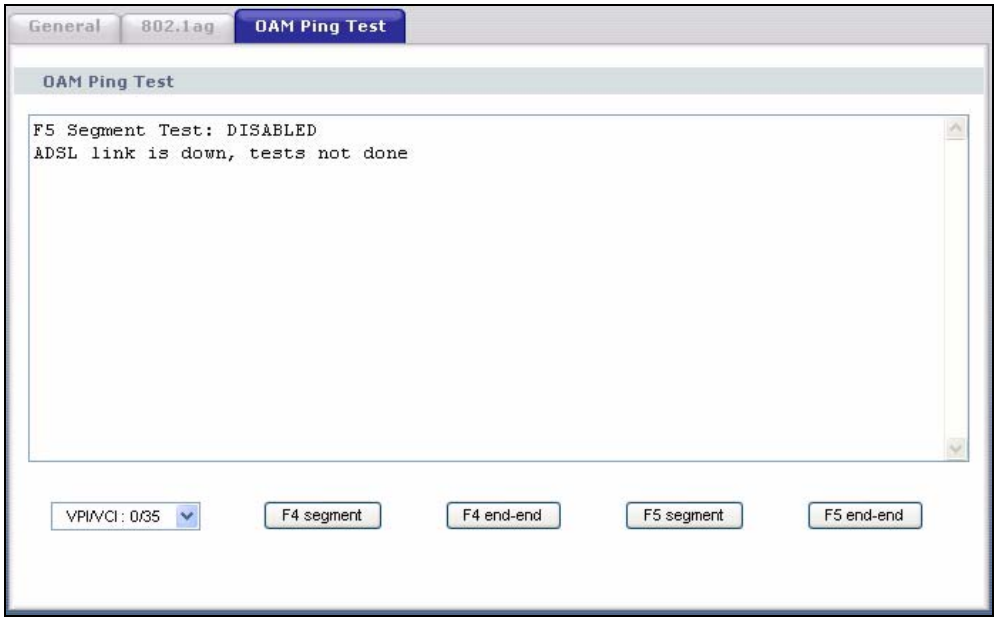
OAM F4 or F5 tests are used to check virtual path or virtual channel availbility between two DSL devices. Segment flows are terminated at the connecting point

which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the P-2812HNU-51c is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface.

Figure 201 Maintenance > Diagnostic > OAM Ping Test



The following table describes the fields in this screen.

Table 137 Maintenance > Diagnostic > OAM Ping Test

LABEL	DESCRIPTION
	Select a PVC on which you want to perform the loopback test.
F4 segment	Press this to perform an OAM F4 segment loopback test.
F4 end-end	Press this to perform an OAM F4 end-to-end loopback test.
F5 segment	Press this to perform an OAM F5 segment loopback test.
F5 end-end	Press this to perform an OAM F5 end-to-end loopback test.

30

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- P-2812HNU-51c Access and Login
- Internet Access
- Phone Calls and VoIP
- USB Device Connection
- Wireless LAN Troubleshooting
- UPnP

30.1 Power, Hardware Connections, and LEDs

The P-2812HNU-51c does not turn on. None of the LEDs turn on.

1. Make sure the P-2812HNU-51c is turned on.
2. Make sure you are using the power adaptor or cord included with the P-2812HNU-51c.
3. Make sure the power adaptor or cord is connected to the P-2812HNU-51c and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the P-2812HNU-51c off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.6 on page 30.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the P-2812HNU-51c off and on.
5. If the problem continues, contact the vendor.

30.2 P-2812HNU-51c Access and Login

I forgot the IP address for the P-2812HNU-51c.

1. The default IP address is **192.168.1.1**.
2. If you changed the IP address and have forgotten it, you might get the IP address of the P-2812HNU-51c by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the P-2812HNU-51c (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 29.

I forgot the password.

1. The default admin password is **1234** and the default user password is **user**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 29.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is **192.168.1.1**.
   - If you changed the IP address (Section on page 144), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the P-2812HNU-51c.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix C on page 445.
4. Reset the device to its factory defaults, and try to access the P-2812HNU-51c with the default IP address. See Section 1.5 on page 29.
5. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

   Advanced Suggestions

   - If your computer is connected to the WAN port or is connected wirelessly, use a computer that is connected to an **ETHERNET** port.
   - Try to access the P-2812HNU-51c using another service, such as Telnet. If you can access the P-2812HNU-51c, check the remote management settings and firewall rules to find out why the P-2812HNU-51c does not respond to HTTPS.

I can see the **Login** screen, but I cannot log in to the P-2812HNU-51c.

1. Make sure you have entered the user name and password correctly. The default admin user name is **admin** and default admin password is **1234**. The default user name is **user** and the default user password is **user**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
2. Turn the P-2812HNU-51c off and on.
3. If this does not work, you have to reset the device to its factory defaults. See Section 30.1 on page 385.

I cannot Telnet to the P-2812HNU-51c.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot access the P-2812HNU-51c again after configuring a new interface group.

Make sure your computer is connected to a LAN port in the default group. Otherwise, you need to use the P-2812HNU-51c's LAN IP address for the new group to access the P-2812HNU-51c again.

30.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.6 on page 30.
2. Make sure you entered your ISP account information correctly in the WAN screens. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5 If the problem continues, contact your ISP.

I cannot access the Internet through a DSL connection.

1 Check if you set the **DSL / WAN** switch (on the back of the P-2812HNU-51c) to the **DSL** side to have the P-2812HNU-51c use the DSL port for Internet access.

2 Make sure you configured a proper ATM or PTM layer-2 interface and WAN services with the Internet account information provided by your ISP.

3 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot access the Internet through an Ethernet WAN connection.

1 Check if you set the **DSL / WAN** switch (on the back of the P-2812HNU-51c) to the **WAN** side to have the P-2812HNU-51c use the Ethernet WAN port for Internet access.

2 Make sure you connect the Ethernet WAN port to a DSL modem or router in your netwrok.

3 Make sure you configured a proper Ethernet layer-2 interface and WAN services with the Internet account information provided by your ISP.

4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot connect to the Internet using a second DSL connection.

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

I cannot create multiple connections of the same type.

Your layer-2 interface must be in VLAN MUX Mode or MSC mode to create multiple WAN serivces for each connection.

I cannot access the Internet anymore. I had access to the Internet (with the P-2812HNU-51c), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.6 on page 30.
2. Turn the P-2812HNU-51c off and on.
3. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.6 on page 30. If the P-2812HNU-51c is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving your computer closer to the P-2812HNU-51c if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3. Turn the P-2812HNU-51c off and on.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

30.4 Phone Calls and VoIP

The telephone port won't work or the telephone lacks a dial tone.

1. Check the telephone connections and telephone wire.
2. Make sure you have the **VoIP > SIP Account** and **SIP Service Provider** screens properly configured. The **PHONE** light should be on when the SIP line is properly registered.

I can access the Internet, but cannot make VoIP calls.

1. Make sure you have the **VoIP > SIP Account** and **SIP Service Provider** screens properly configured.
2. The **PHONE** light should come on. Make sure that your telephone is connected to the **PHONE** port.
3. You can also check the VoIP status in the **Status** screen.

30.5 USB Device Connection

The P-2812HNU-51c fails to detect my USB device.

1. Disconnect the USB device.
2. Reboot the P-2812HNU-51c.
3. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
4. Re-connect your USB device to the P-2812HNU-51c.

30.6 Wireless LAN Troubleshooting

I cannot access the P-2812HNU-51c or ping any computer from the WLAN (wireless AP or router).

1. Make sure the wireless LAN is enabled on the P-2812HNU-51c.
2. Make sure the wireless adapter on the wireless station is working properly.
3. Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the P-2812HNU-51c.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the P-2812HNU-51c.
5. Check that both the P-2812HNU-51c and your wireless station are using the same wireless and wireless security settings.
6. Check if MAC Filter is configured to deny wireless access to certain MAC addresses to the P-2812HNU-51c. See Chapter 7 Wireless LAN in the User's Guide for more information.

I cannot use WDS connection.

1. You can use WDS only when WPS is disabled or wireless security is set to "No Security", "WEP", "WPA-PSK" or "WPA2-PSK". The wireless security settings apply to both WDS links and the connections between the P-2812HNU-51c and any wireless clients.
2. WDS is only compatible with other ZyXEL Devices of the same model.

30.7 UPnP

When using UPnP and the P-2812HNU-51c reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1 Disconnect the Ethernet cable from the P-2812HNU-51c's LAN port or from your computer.

2 Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

1 Wait more than three minutes.

2 Restart the applications.

31

Product Specifications

The following tables summarize the P-2812HNU-51c's hardware and firmware features.

31.1 Hardware Specifications

Table 138 Hardware Specifications

Dimensions	240 (W) x 170 (D) x 60 (H) mm
Weight	420 g
Power Specification	12 V DC 2A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100/1000 Mbps RJ-45 Ethernet ports
RESET Button	Restores factory defaults
Antennas	One attached external dipole antenna, 2dBi One internal antenna , 2dBi
WPS Button	1 second: turn on or off WLAN 5 seconds: enable WPS (Wi-Fi Protected Setup)
PHONE Ports	2 RJ-11 FXS POTS ports
USB Ports	Two USB v2.0 ports for file sharing
Operation Temperature	0º C ~ 40º C
Storage Temperature	-30º ~ 60º C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH

31.2 Firmware Specifications

Table 139 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default User Name	admin
Default Password	1234
DHCP Server IP Pool	192.168.1.33 to 192.168.1.132
Static Routes	16
Device Management	Use the web configurator to easily configure the rich range of features on the P-2812HNU-51c.
Wireless Functionality (wireless devices only)	Allow the IEEE 802.11b, IEEE 802.11g and/or IEEE 802.11n wireless clients to connect to the P-2812HNU-51c wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator to put it on the P-2812HNU-51c. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the P-2812HNU-51c's configuration. You can put it back on the P-2812HNU-51c later if you decide to revert back to an earlier configuration.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the P-2812HNU-51c assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The P-2812HNU-51c supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your P-2812HNU-51c. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the P-2812HNU-51c to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

Table 139 Firmware Specifications (continued)

QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTPS or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the P-2812HNU-51c.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
Packet Filters	Your device's packet filtering function allows added network security and management.
VDSL Standards	VDSL line coding: ITU-T G.993.2 DMT modulation DSL handshake procedure protocol: ITU-T G.994.1 DSL physical layer management protocol: ITU-T G.997.1 VDSL band plan: 997 and 998 Support U0 band VDSL profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a VDSL speed: up to 100/50 Mbps@ 700 feet Support Annex A, Annex B and 5-band VDSL2 Rate adaptation OLR: Bit Swapping/ SRA (Seamless Rate Adaption) Upstream power back-off (UPBO) VDSL OAM communication channels: Indicator bits (IB) channel, VDSL embedded operations channel (EOC) and VDSL overhead control channel (VOC) PTM Transmission Convergence (PTM-TC) Dual-latency xDSL framing (fast and interleaved) Trellis coding INP capability: At least two symbols protection (INP_MIN = 2), up to 16 symbols (INP_MIN = 16)

Table 139 Firmware Specifications (continued)

ADSL Standards	Multi-Mode standard (ANSI T1.413,Issue 2; G.dmt(G.992.1); G.lite(G992.2)) ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC 2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) MAC encapsulated routing (ENET encapsulation) VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) I.610 F4/F5 OAM
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol Transparent bridging for unsupported network layer protocols RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy
Management	Embedded Web Configurator Remote Firmware Upgrade SNMP v1 & v2c with MIB II Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore Syslog TR-069 TR-064
Supported Operating Systems	• Windows 7/Vista/XP/2000 • Mac OS 9/OS X

The following list, which is not exhaustive, illustrates the standards supported in the P-2812HNU-51c.

Table 140 Standards Supported

STANDARD	DESCRIPTION
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2364	PPP over AAL5 (PPP over ATM over ADSL)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/ WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard.
G dmt(G.992.1)	G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers
ITU G.992.1 (G.DMT)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.2 (G. Lite)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.4 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits.
ITU-T G.993.2 (VDSL2)	ITU standard that defines VDSL2.
TR-069	DSL Forum Standard for CPE Wan Management.
TR-064	DSL Forum LAN-Side DSL CPE Configuration

A

Network Troubleshooting

Overview

The three most basic utilities for troubleshooting network connection issues are: `ipconfig`, `ping` and `tracert`. This appendix gives a quick overview of them as well as some common usage examples. Moreover, three slightly more advanced utilities are also discussed: `arp`, `route`, and `netstat`.

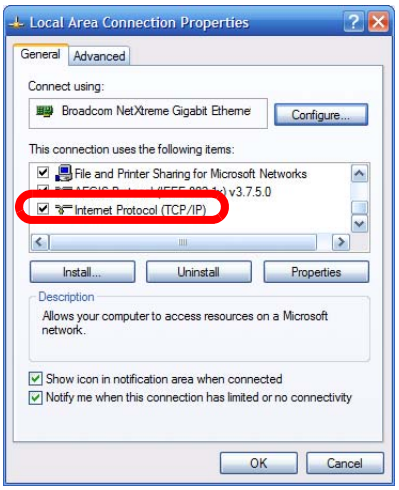
Note: All command examples here use the Microsoft Windows operating system version of the commands.

Before Getting Started

Before using the commands described in this section, ensure that you have the TCP/IP networking component installed and properly configured for your network adapter.

Click **Start > Control Panel > Network Connections** and then open a **Local Area Connection** to display the following screen.

Figure 202 TCP/IP Networking Component



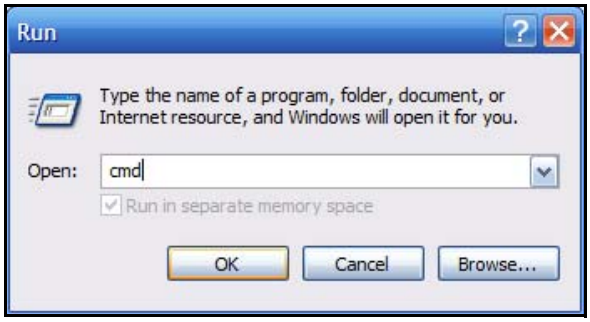
Note: Most operating systems ship with TCP/IP already installed and enabled. See your Windows documentation for details on installing or configuring TCP/IP.

The Command Line Interface

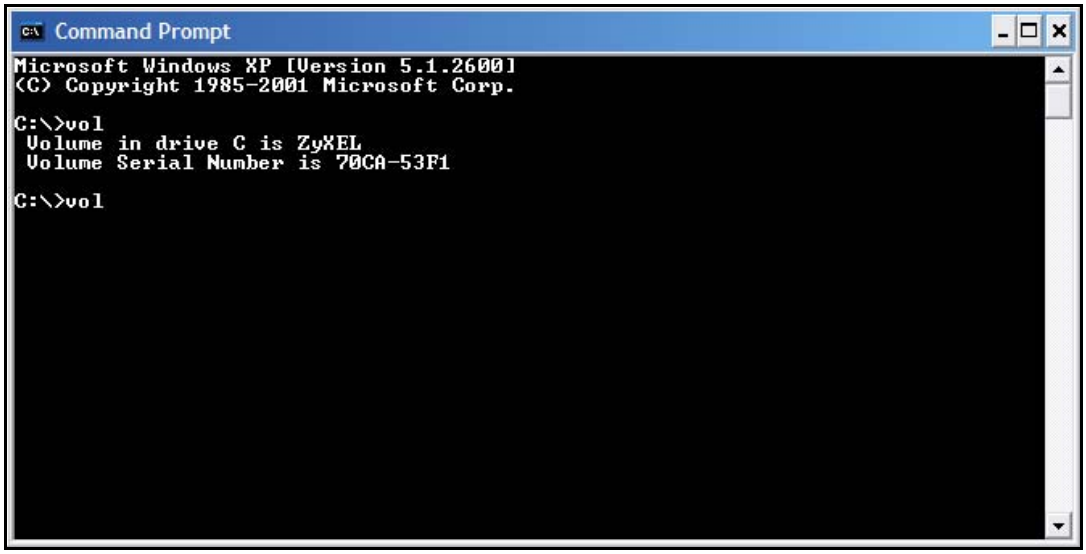
To open the Windows command line interface:

1 Click **Start > Run**.

2 In the **Run** dialog box, enter **cmd** then click **OK**.



3 The **Command Prompt** window opens.



Command Syntax and Parameters

Command descriptions always indicate the default syntax you must use when entering them on the command line. Some commands require additional parameters in order to execute properly. Some may have optional parameters.

Parameters are displayed as follows: `command [parameter]`

For example, the date command has the optional /t and date parameters. If you do not use either of them and enter just date by itself, then the system shows you the date it is currently using and then prompts you to change it.

```
C:\>date
The current date is: 2009/10/21
Enter the new date: (mm-dd-yy)
```

However, if you use the /t parameter it just displays the date and nothing more.

```
C:\>date /t
2009/10/21

C:\>
```

To view the parameters for any given command, enter help [command].

ipconfig

The ipconfig command line utility allows you to display current network (TCP/IP) configuration settings and, in some cases, adjust them. When you have network connectivity problems, the first thing you should do is run this command to ensure that your device or computer does in fact have an IP address as well as display the source of that IP address (such as a default gateway).

Syntax: ipconfig

Parameters: ipconfig [/release] [/renew]

There are other parameters, but these are the only ones you need to use for now.

The following examples show the typical output of this command:

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : example.com
        IP Address. . . . . . . . . . . . : 192.168.1.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 1.1.1.4

C:\>
```

Here you can see that the device has IP address of 1.1.1.1 and example.com is its Domain Name Server (DNS).

If the device is disconnected then you would see the following instead:

```
Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected
```

If the device is connected but cannot get an IP address then you would see:

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :
```

In some cases, your computer may be properly connected to the network or the P-2812HNU-51c but it is not receiving an IP address for whatever reason. Use the `/release` parameter followed by `/renew`:

```
C:\>ipconfig /release

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : zyxel.com
        IP Address. . . . . . . . . . . . : 192.168.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 2.2.2.4

C:\>
```

ping

The ping command line utility allows you to verify the connection and latency between your computer and either the P-2812HNU-51c or other devices on the network. If you cannot reach a target using this command, then it may indicate possible network trouble.

Syntax: ping *target*

The *target* can be an IP address or a host name.

Parameters: ping [-w *timeout*] *target*

The *timeout* parameter allows you to input the number of seconds (in milliseconds) that your computer waits for a reply.

The following examples show the typical output of this command:

```
C:\>ping www.zyxel.com

Pinging a1524.g.akamai.net [203.69.113.18] with 32 bytes of data:

Reply from 203.69.113.18: bytes=32 time=6ms TTL=56
Reply from 203.69.113.18: bytes=32 time=6ms TTL=56
Reply from 203.69.113.18: bytes=32 time=6ms TTL=56
Reply from 203.69.113.18: bytes=32 time=7ms TTL=48

Ping statistics for 203.69.113.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 7ms, Average = 6ms

>
```

The number of bytes here indicates packet size. As most data is broken up into smaller packets, this makes the ping test fairly representative of a typical network connection. The default packet size on Windows is 32 bytes.

Time is the number of milliseconds the data requires to make the roundtrip journey from your computer to the destination host and back again. The lower the number, the faster the connection between the two points.

Note: Some hosts are deliberately configured to not respond to ping requests. As such, we suggest pinging two or three hosts when performing your ping test.

If your ping test fails to get a response, then you may see a message like this:

```
C:\>ping www.example.com

Pinging www.example.com [192.0.32.10] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.0.32.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

When a request times out it may mean:

- your computer is not connected to the network
- your Internet access device is not connected to the network
- or the device which you are pinging is not connected to the network

If you think the destination is active but responding slowly, you can try increasing the ping timeout value from its default of 4 seconds (4000 milliseconds) to something like 8 seconds (or 8000 milliseconds).

```
C:\>ping -w 8000 www.example.com

Pinging www.example.com [192.0.32.10] with 32 bytes of data:

Reply from 192.0.32.10: bytes=32 time=157ms TTL=238
Reply from 192.0.32.10: bytes=32 time=154ms TTL=238
Reply from 192.0.32.10: bytes=32 time=152ms TTL=236
Reply from 192.0.32.10: bytes=32 time=162ms TTL=236

Ping statistics for 192.0.32.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 152ms, Maximum = 162ms, Average = 156ms

C:\>
```

A long ping response could indicate network problems:

- on your side of the connection
- between the start and end points of the connection
- on the receiving end

To determine where the slowdown is, you may need to use traceroute.

tracert

The `tracert` command line utility allows you to determine the network path between your computer and a host you specify. When you communicate with other devices on a network, the data is not often sent directly from point A to point B; rather, it moves through a series of intermediate servers, passed along until eventually the server closest to point B hands it off directly. This command can be useful for helping determine whether your connection issues are happening locally, somewhere in transit, or at the destination end.

- Each step in the chain of connections is called a 'hop'.
- The time it takes for a server at any given hop to pass the data packet is called 'latency' and is measured in milliseconds.

When a `tracert` command is run, it sends out a burst of three data packets per hop. The results table, therefore, always displays three values for latency in addition to the IP address and domain name (where available) of the server on that leg of the journey.

Syntax: `tracert` *`target`*

The `target` can be an IP address or a host name.

Parameters: `tracert [-d] [-h` *`maximumhops`* `]` *`target`*

There are other parameters but these are the only ones you need to use for now.

The following examples show the typical output of this command:

```
C:\>tracert www.example.com

Tracing route to www.example.com [192.0.32.10]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.23.x.x
  2     5 ms     4 ms     5 ms  172.23.x.x
  3     4 ms     4 ms     4 ms  172.23.x.x
  4     5 ms     4 ms     6 ms  219-87-158-97.static.tfn.tw [219.87.158.97]
  5     6 ms     5 ms     4 ms  10.42.232.150
  6     5 ms     4 ms     4 ms  hc-c12r2.router.tw [220.128.7.86]
  7    10 ms     7 ms    10 ms  tp-s2-c12r12.router.tw [220.128.2.90]
  8     9 ms     7 ms     8 ms  pr03-s2.tp.tw [220.128.4.181]
  9     6 ms     6 ms     9 ms  220-128-3-249.NET-IP.tw [220.128.3.249]
 10   138 ms   137 ms   138 ms  r11-pa.NET-IP.net [211.72.108.129]
 11   138 ms   138 ms   138 ms  po4-0.core01.sjc04.atlas.com [154.54.11.129]
 12   128 ms   139 ms   140 ms  te9-2.mpd01.sjc04.atlas.com [154.54.0.173]
 13   140 ms   139 ms   136 ms  61.58.33.173
 14   154 ms   153 ms   137 ms  xe-0-0-0.r20.gin.ntt.net [129.250.16.161]
 15   154 ms   154 ms   137 ms  as-2.r21.tokyjp01.jp.ntt.net [129.250.4.81]
 16   562 ms   553 ms   553 ms  38.106.6.34
 17   554 ms   554 ms   553 ms  po-2.r00.lsanca19.us.ntt.net [129.250.6.42]
 18   254 ms   254 ms   248 ms  204.1.254.150
 19   154 ms   253 ms   154 ms  192.0.32.10

Trace complete.

C:\>
```

Here, the `tracert` to www.example.com took 18 hops to reach its destination. Looking at the latency data, you'll see the first slow down happens at hop 10.

The extremely low latency on the first few hops indicates a network local to the computer where the `tracert` command originated, such as a home or office LAN. The packets then move onto the local WAN (such as your Internet Service Provider's network). Because of the close proximity of those servers to your computer, the latency remains low.

Once the data packets move out of the regional network to the first international server (at hop 10 in this example), the latency increases. This is because of the distance between the regional and international servers - it physically takes longer for the response to get back to your computer.

Finally, on transition hop 15 from the server in Japan to the server in California, another latency spike occurs. If you were having connection problems, this would most likely be the source of it. For whatever reason, the server in Japan has a less than optimal connection with its counterpart in the United States.

In this example, we abridge the `tracert` results table to show only server IP addresses and not domain names by using the `-d` parameter. We also use the `-h` parameter to limit the number of hops to 5 to test local connections only.

```
C:\>tracert -d -h 5 www.zyxel.com

Tracing route to a1524.g.akamai.net [203.69.113.16]
over a maximum of 5 hops:

  1    <1 ms    <1 ms    <1 ms  172.23.31.254
  2     5 ms     4 ms     4 ms  172.23.6.113
  3     5 ms     5 ms     6 ms  172.23.6.253
  4    17 ms    16 ms    14 ms  218.160.188.254
  5    24 ms    25 ms    24 ms  10.42.232.150

Trace complete.

C:\>
```

arp

Local network transmission is based on MAC addresses. Data transmission between two networks is based on IP addresses.

Address Resolution Protocol (ARP) is a protocol that converts IP addresses into MAC addresses. Before a computer transmits data to an IP address on the same network, it will check whether the IP address exists in its ARP table. If it does, the computer then sends the data directly to the mapped MAC address. If it does not, the computer broadcasts an ARP request to the network. The host whose MAC address maps to the IP address responds.

When you use `ping` to check the connection to a computer, no response does not mean the computer is not alive on the network. The destination computer may be configured not to respond to any ping requests. However, you can use the `arp -a` command line utility to check the IP addresses and MAC addresses of your neighboring computers or devices.

Syntax: `arp -a`

Parameters: `arp [-d` *`inet_addr`*`] [-s` *`inet_addr eth_addr`*`]`

The `-d` parameter can be use alone to remove all entries from an arp table or in conjunction with an IP address to remove just that IP address (*`inet_addr`*). The `-s` parameter allows you to add entries based on IP address (*`inet_addr`*) and/or MAC address (*`eth_addr`*).

There are other parameters but these are the only ones you need to use for now.

To check the ARP table on a Windows XP computer:

1 Click **Start** > **Programs** > **Accessories** > **Command Prompt**. The **Command Prompt** screen appears.

2 Type `arp -a` and press `[Enter]`.

The following examples show the typical output of this command:

```
C:\>arp -a
Interface: 172.16.1.28 on Interface 0x1000003
  Internet Address      Physical Address      Type
  172.16.1.5            00-00-aa-19-07-38     dynamic
  172.16.1.25           00-18-f3-f0-aa-34     dynamic
  172.16.1.44           00-0e-a6-2c-60-10     dynamic
  172.16.1.210          00-19-cb-e9-66-33     dynamic
  172.16.1.254          00-04-80-4c-a8-05     dynamic
```

In this example, the **Physical Address** indicates the associated MAC address. A **Type** entry with **dynamic** means it was dynamically learned through an ARP response. Use the `arp -s [inet_addr eth_addr]` to manually add an ARP entry if you want your computer to connect to the host with the specified MAC address when you access the specified IP address.

You can additionally check whether the MAC address associated with the IP address that you are looking for is correct. In some circumstances, your ARP table may keep a wrong MAC address until the entry expires. You can then manually update the ARP table.

To update the ARP table:

1 Type `arp -d [inet_addr]` or just use `arp -d` to remove all entries in the ARP table. For example, type `arp -d 172.16.1.5`.

2 Type `ping 172.16.1.5` and press `[Enter]`.

3 Next, use the `arp -a` command again to check whether the MAC address matches what you expected. If it does not, another computer may be using a duplicate IP address on the network. Change the IP address on either computer to an unused one to fix this problem.

route

The `route` command line utility allows you to display or adjust your computer's network table. The routing table on your computer contains the default gateway

and other route information. When your computer wants to access an IP address on another network, it references this table.

Syntax: `route print`

Parameters: For the purposes of this section, the *print* parameter is the most important. If you enter `route` by itself, the command's help page displays.

The following example shows the typical output of this command:

```
C:\>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 02 e3 a1 b2 c3 ...... Broadcom NetXtreme Gigabit Ethernet
Driver

===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     172.16.1.254    172.16.1.32       1
        127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1       1
       172.16.1.0    255.255.255.0      172.16.1.32    172.16.1.32       1
      172.16.1.32  255.255.255.255        127.0.0.1      127.0.0.1       1
   172.16.255.255  255.255.255.255      172.16.1.32    172.16.1.32       1
        224.0.0.0        224.0.0.0      172.16.1.32    172.16.1.32       1
  255.255.255.255  255.255.255.255      172.16.1.32    172.16.1.32       1
Default Gateway:     172.16.1.254
===========================================================================
Persistent Routes:
  None
```

The following table describes labels shown in the command output:

Table 141 route print Command Output

OUTPUT	DESCRIPTION
Active Routes	This section lists all available routes that are automatically learned from the network.
Network Destination	The destination IP address of packets that this route entry is to route. The destination can be an IP address for a network or host, 0.0.0.0 for the default route or 127.0.0.0 for the loopback interface which is used mainly for self-test. The destination 224.0.0.0 is for multicasting packets or reserved for testing. But if you are not using multicast applications, just ignore it. The destination 255.255.255.255 is used to find computers when an IP address is not known. For example, before the DHCP IP address of your computer is determined, your computer sends packets with the destination looking for DHCP servers on the network.

Table 141 route print Command Output

OUTPUT	DESCRIPTION
Netmask	The destination subnet mask of packets that this route entry is to route. The subnet mask can be the apropriate subnet mask for a network, 255.255.255.255 for a host, or 0.0.0.0 for the default route.
Gateway	The IP address of the gateway through which this computer should send the matched packets.
Interface	The IP address of an physical interface on this computer used to send the matched packets for this route entry.
Metric	The metric (hop count) of this route. Normally, the lower the number, the faster to a destination.
Default Gateway	The IP address of the gateway through which this computer sends all the rest packets if this computer cannot find any other matched routes for the packets.
Persistent Routes	This section lists all routes that are manually configured.

In this example, the 172.16.1.0 is the network address. The 172.16.1.32 is the address of the local computer. 172.16.1.255 is the network broadcast address which sends broadcast packets to all computers on the 172.16.1.x network. 172.16.1.254 is the default gateway.

You may have more than one 0.0.0.0 entry if your computer has two or more network cards installed. This may casue packets to be routed somewhere unexpected. Delete all 0.0.0.0 entries except the one that you want to use for the default gateway. In the following example, the computer uses the first 0.0.0.0 entry for the default gateway.

```
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.254    192.168.1.33       1
          0.0.0.0          0.0.0.0     172.16.1.254     172.16.1.32       1
```

- To delete the route to the default route with the gateway of 192.168.1.254, type: `route delete 0.0.0.0 mask 0.0.0.0 192.168.1.254`.
- To add a route to the destination 172.16.2.0 with the subnet mask of 255.255.255.0, the next hop address of 172.16.1.250, and the cost metric of 7, type: `route add 172.16.2.0 mask 255.255.255.0 172.16.1.250 metric 7`.
- To add a persistent route to the destination 172.16.3.0 with the subnet mask of 255.255.255.0 and the next hop address of 172.16.1.252, type: `route -p add 172.16.3.0 mask 255.255.255.0 172.16.1.252`.

Note that the metric will be set to 1 if you do not specify any.

netstat

The netstat command line utility is used to show Ethernet statistics and current TCP/IP network connections.

Syntax: netstat

With no parameters, this command simply displays only active statistics for ports that are currently in use by one process or another.

Parameter: netstat [-a] [-e]

The -a parameter displays all available listening ports and connections whether they are active or not, while the -e parameter displays Ethernet statistics.

There are other parameters but these are the only ones you need to use for now.

The following examples show the typical output of this command:

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    COMPUTERA:1056         localhost:5091         ESTABLISHED
  TCP    COMPUTERA:1091         localhost:27015        ESTABLISHED
  TCP    COMPUTERA:1120         localhost:40000        ESTABLISHED
  TCP    COMPUTERA:3243         localhost:3244         ESTABLISHED
  TCP    COMPUTERA:3244         localhost:3243         ESTABLISHED
  TCP    COMPUTERA:3246         localhost:3247         ESTABLISHED
  TCP    COMPUTERA:3247         localhost:3246         ESTABLISHED
  TCP    COMPUTERA:5091         localhost:1056         ESTABLISHED
  TCP    COMPUTERA:5152         localhost:3245         CLOSE_WAIT
  TCP    COMPUTERA:27015        localhost:1091         ESTABLISHED
  TCP    COMPUTERA:40000        localhost:1120         ESTABLISHED
  TCP    COMPUTERA:3229         172.20.0.201:http      CLOSE_WAIT
  TCP    COMPUTERA:3234         172.16.1.29:1155       ESTABLISHED
  TCP    COMPUTERA:3237         172.16.1.29:1155       ESTABLISHED
  TCP    COMPUTERA:3240         172.16.1.29:1155       ESTABLISHED

C:\>
```

Use the -a parameter to display all possible connections to your device, not just the ones that are currently in use:

```
C:\>netstat -a
Active Connections

  Proto  Local Address          Foreign Address          State
  TCP    COMPUTERA:http         COMPUTERA:0              LISTENING
  TCP    COMPUTERA:http         172.16.x.x:4036          ESTABLISHED
  TCP    COMPUTERA:2744         NAS:microsoft-ds         ESTABLISHED
  TCP    COMPUTERA:5152         172.16.x.x.ZyXEL.com:0   LISTENING
  TCP    COMPUTERA:5152         localhost:4067           CLOSE_WAIT
  TCP    COMPUTERA:5354         172.16.x.x.ZyXEL.com:0   LISTENING
  TCP    COMPUTERA:27015        172.16.x.x.ZyXEL.com:0   LISTENING
  TCP    COMPUTERA:40000        localhost:0              LISTENING
  TCP    COMPUTERA:40000        localhost:1120           ESTABLISHED
  TCP    COMPUTERA:netbios-ssn  172.16.x.x.ZyXEL.com:0   LISTENING
  TCP    COMPUTERA:4177         172.16.x.x:1155          ESTABLISHED
  TCP    COMPUTERA:4178         172.16.x.x:1155          ESTABLISHED
  TCP    COMPUTERA:4180         172.16.x.x:1155          ESTABLISHED
  TCP    COMPUTERA:4182         172.16.x.x:1025          ESTABLISHED
  TCP    COMPUTERA:4317         NAS:microsoft-ds         ESTABLISHED
  TCP    COMPUTERA:4539         NAS:microsoft-ds         TIME_WAIT
  TCP    COMPUTERA:netbios-ssn  172.16.x.x:0             LISTENING
  TCP    COMPUTERA:netbios-ssn  172.16.x.x:0             LISTENING

C:\>
```

The following table describes the three entries in the output example above:

Table 142 netstat -a Command Output

OUTPUT	DESCRIPTION
TCP COMPUTERA:http COMPUTERA:0 LISTENING	A web server is available on **COMPUTERA** as an HTTP service is in a **LISTENING** state.
TCP COMPUTERA:http 172.16.1.29:4036 ESTABLISHED	A computer with an IP address of 172.16.1.29 is accessing the web service on the **COMPUTERA**.
TCP COMPUTERA:2744 NAS:microsoft-ds ESTABLISHED	**COMPUTERA** has established a TCP/IP NETBIOS connection (**microsoft-ds**) with a NAS device.

Additionally, you can use `netstat -e` to display Ethernet statistics as the following example.

```
C:\ >netstat -e
Interface Statistics

                           Received            Sent

Bytes                      25250033         7060325
Unicast packets               38838           34744
Non-unicast packets           38227             175
Discards                          0               0
Errors                            0              35
Unknown protocols               787
```

B

Setting Up Your Computer's IP Address

Note: Your specific P-2812HNU-51c may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

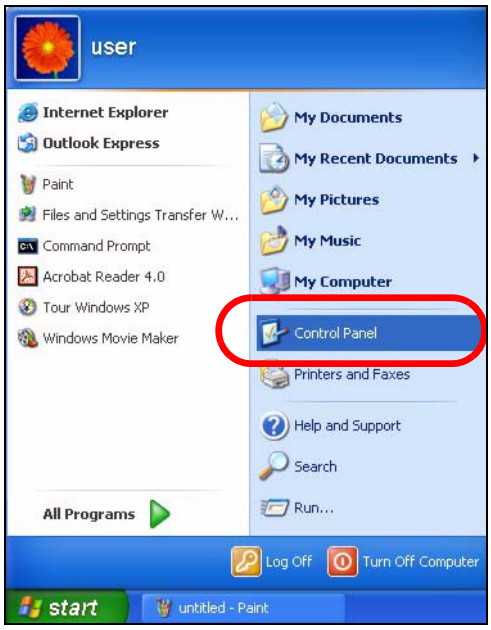
In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 418
- Windows Vista on page 421
- Windows 7 on page 425
- Mac OS X: 10.3 and 10.4 on page 429
- Mac OS X: 10.5 and 10.6 on page 432
- Linux: Ubuntu 8 (GNOME) on page 435
- Linux: openSUSE 10.3 (KDE) on page 440

Windows XP/NT/2000

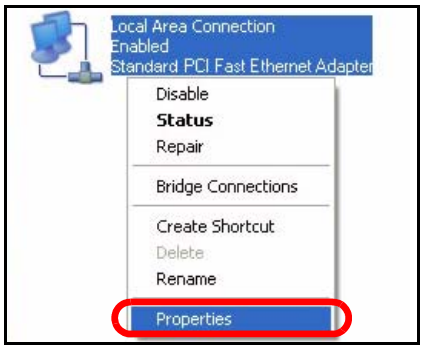
The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

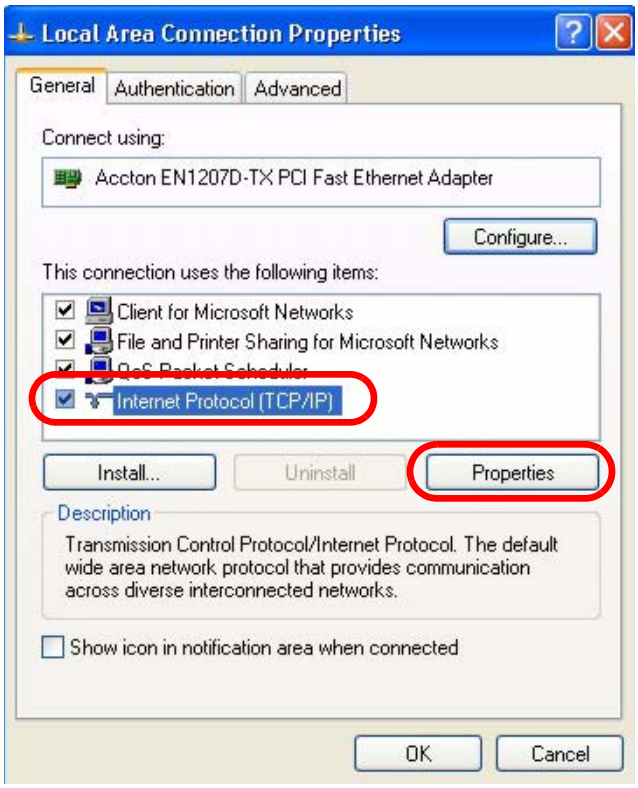


2 In the **Control Panel**, click the **Network Connections** icon.

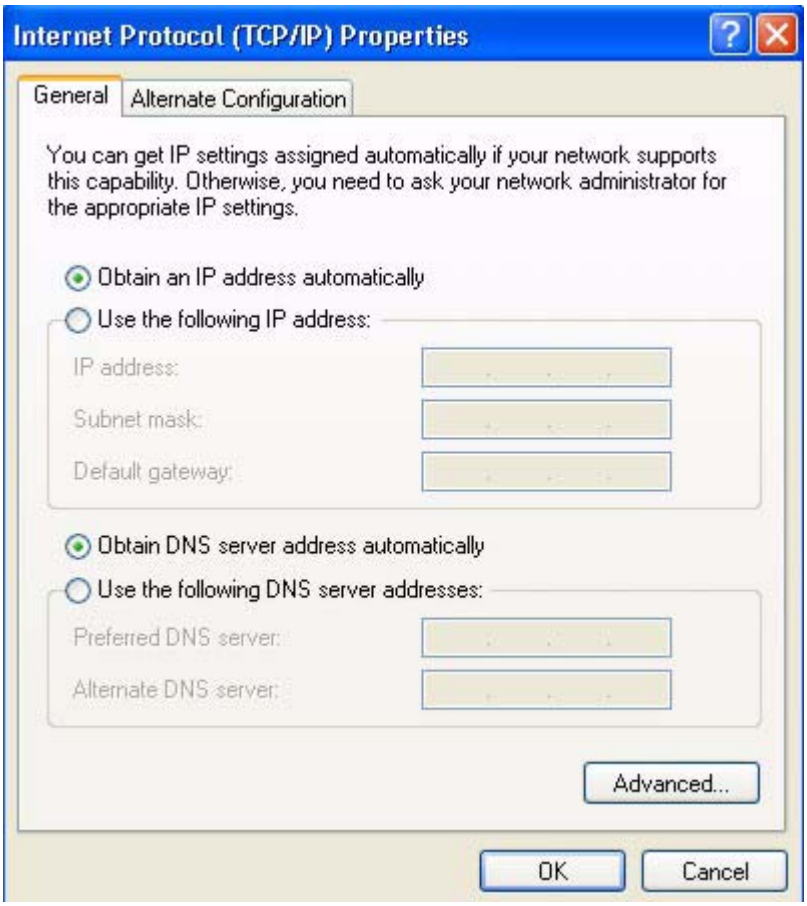
3 Right-click **Local Area Connection** and then select **Properties**.



4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.



5 The **Internet Protocol TCP/IP Properties** window opens.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

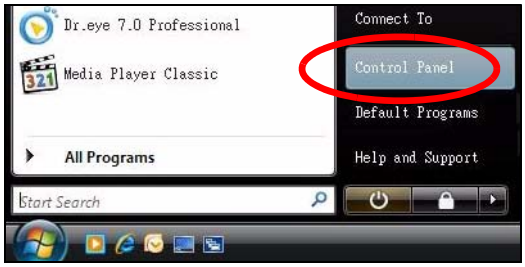
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

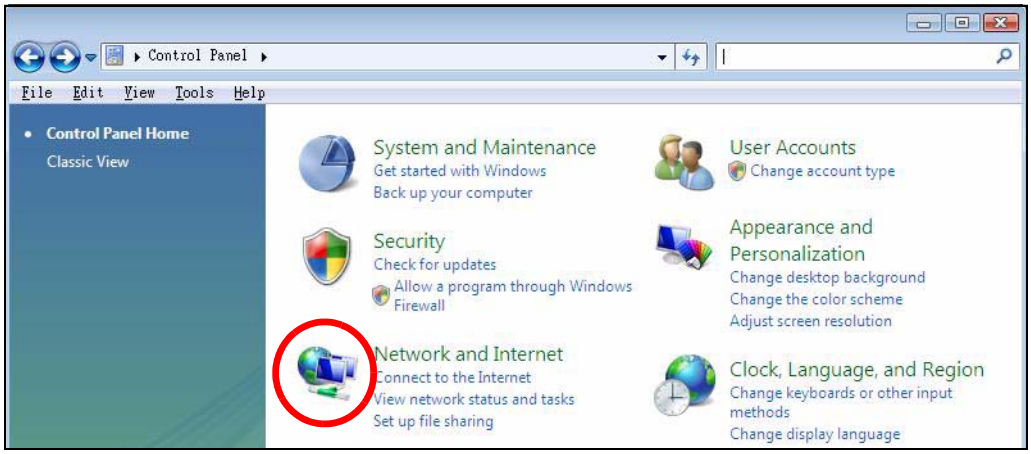
Windows Vista

This section shows screens from Windows Vista Professional.

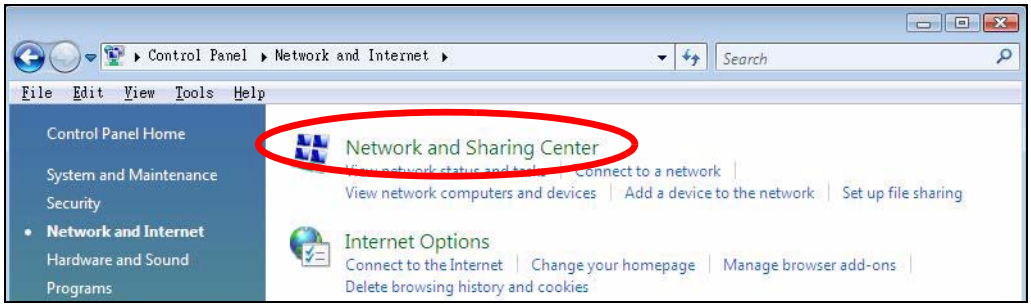
1 Click **Start** > **Control Panel**.



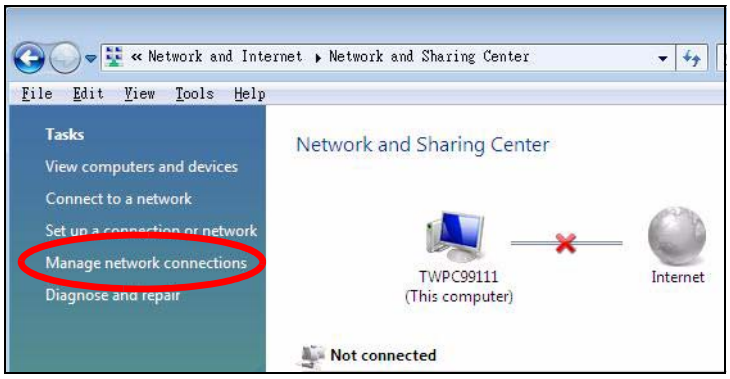
2 In the **Control Panel**, click the **Network and Internet** icon.



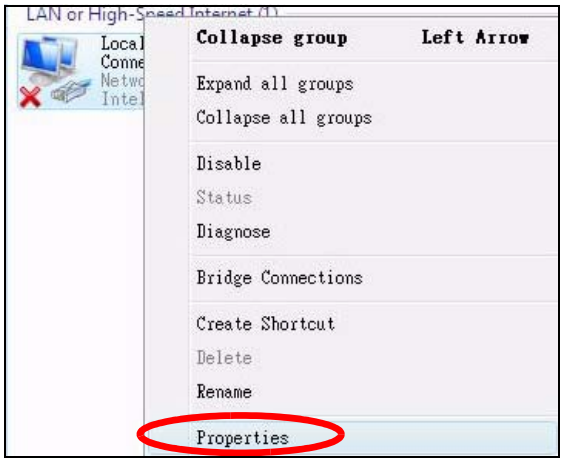
3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

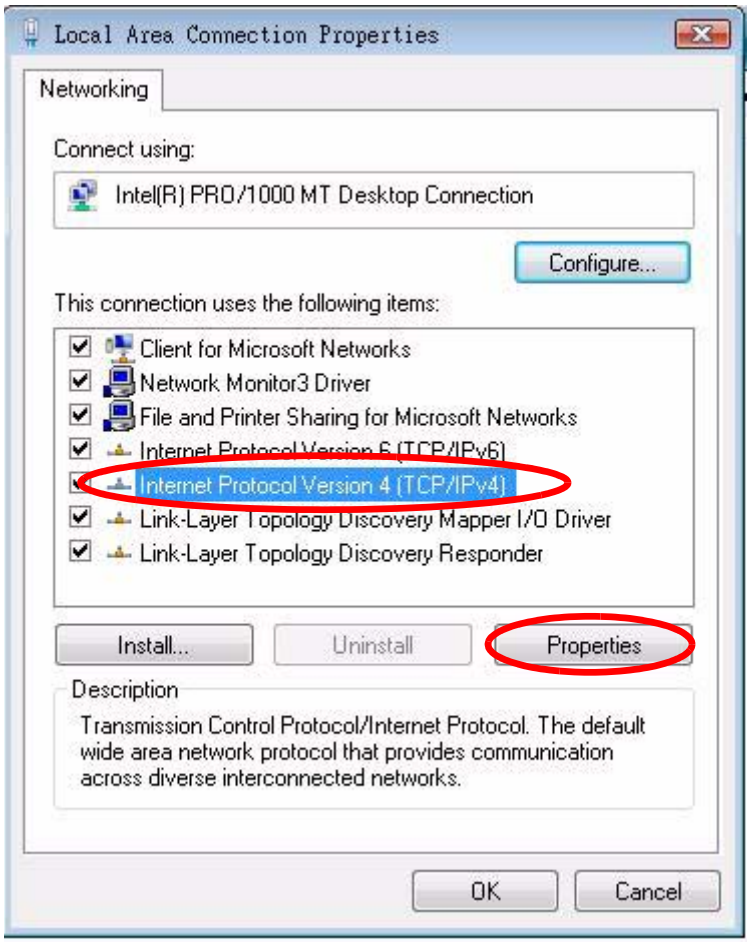


5 Right-click **Local Area Connection** and then select **Properties**.

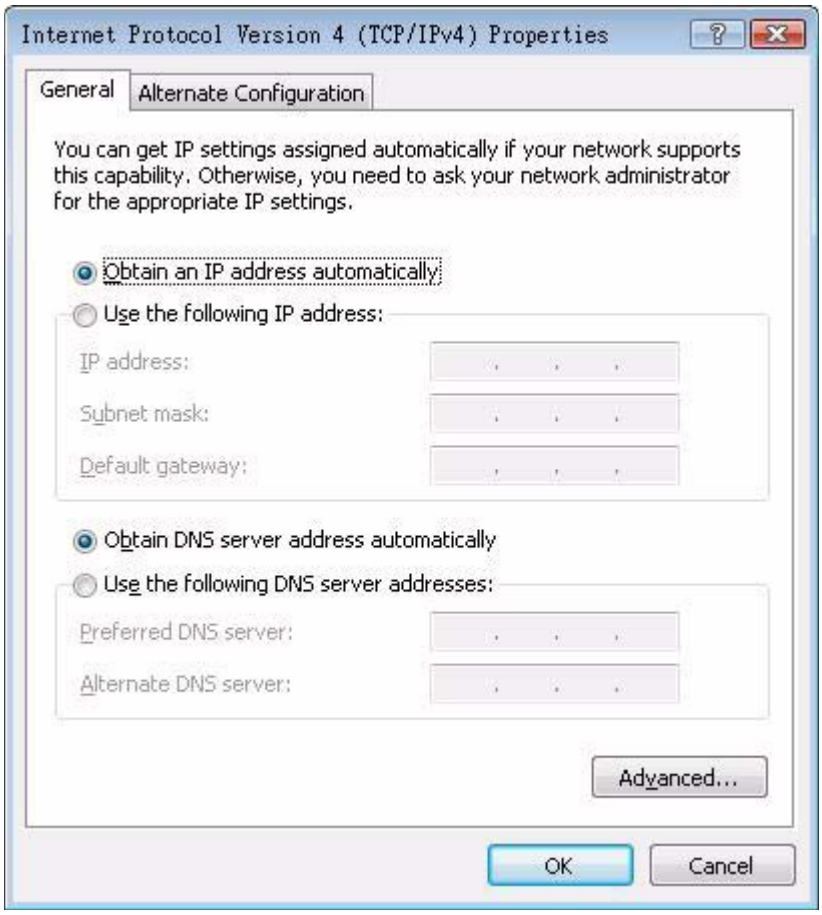


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

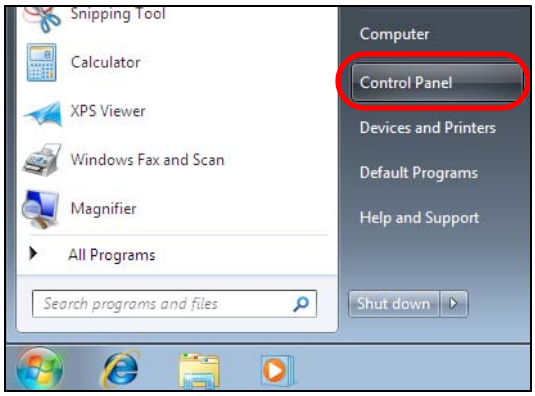
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

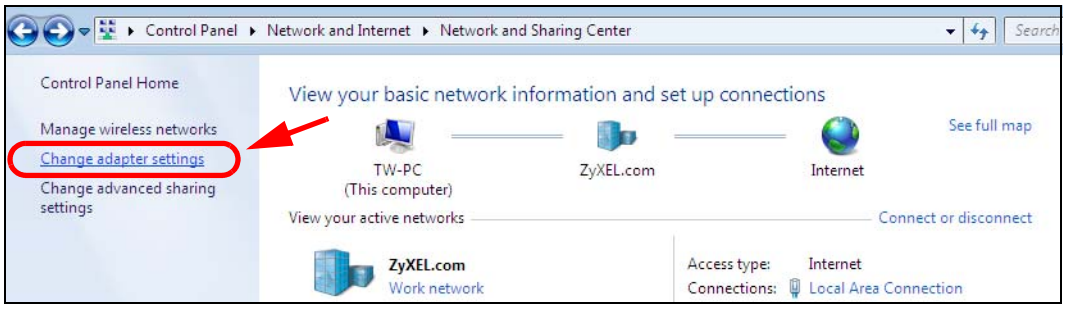
This section shows screens from Windows 7 Enterprise.

1 Click **Start** > **Control Panel**.

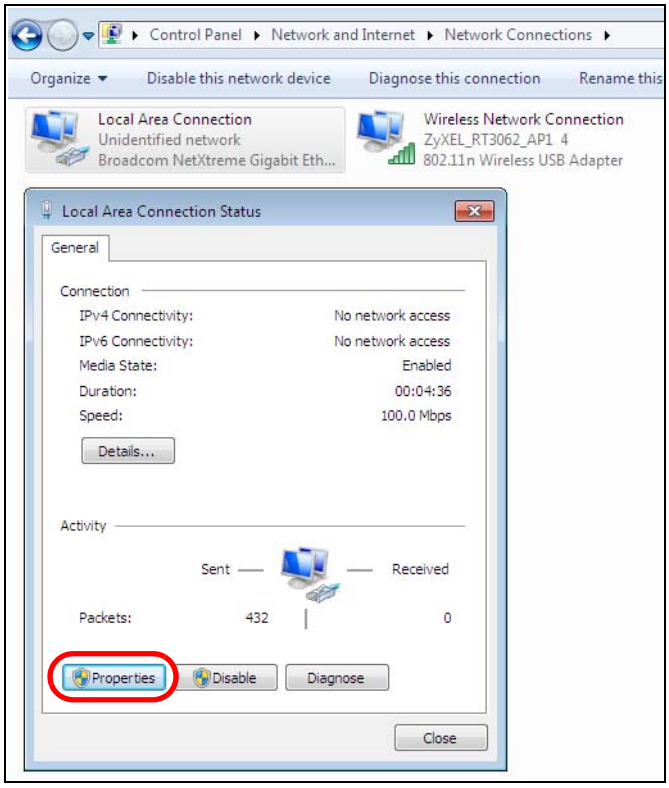


2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

3 Click **Change adapter settings**.

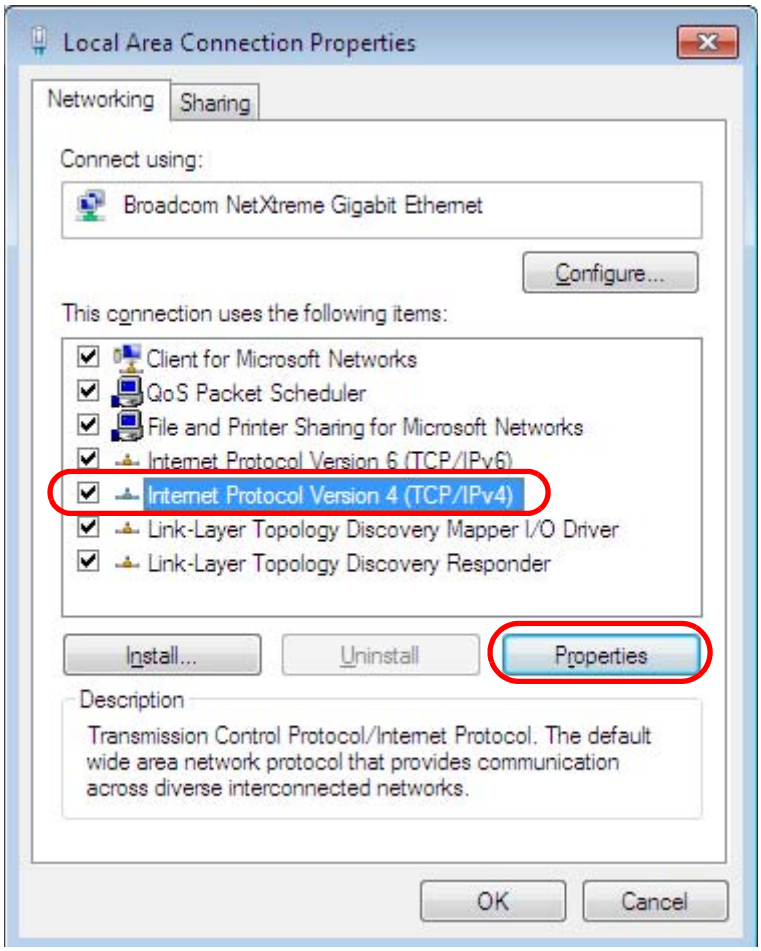


4 Double click **Local Area Connection** and then select **Properties**.

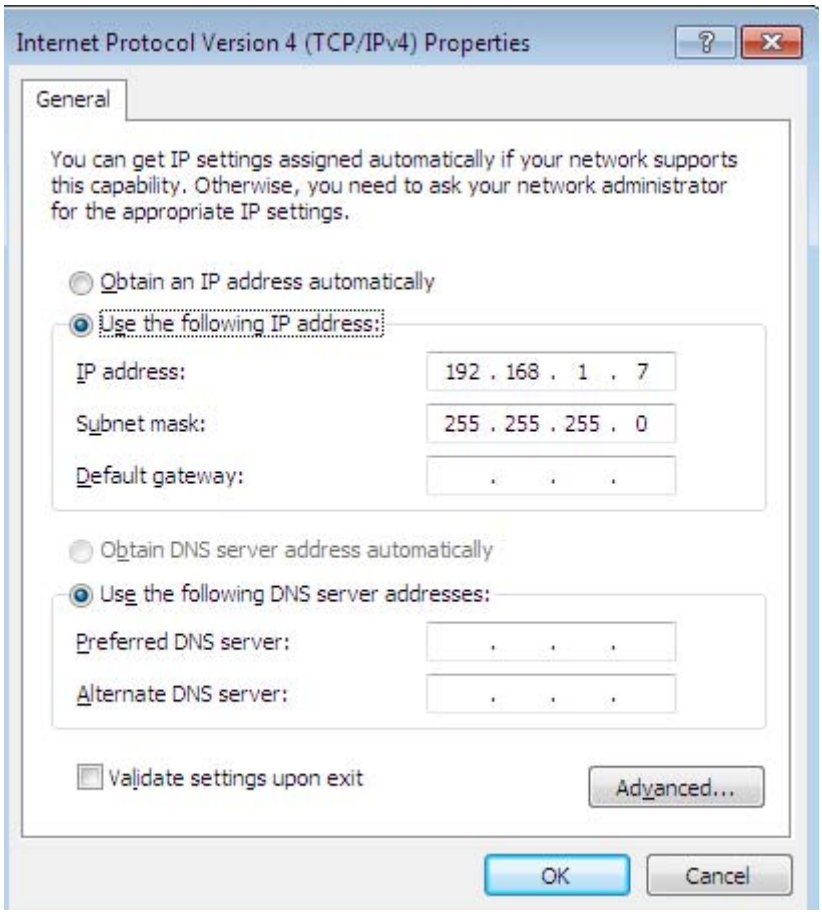


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 7
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

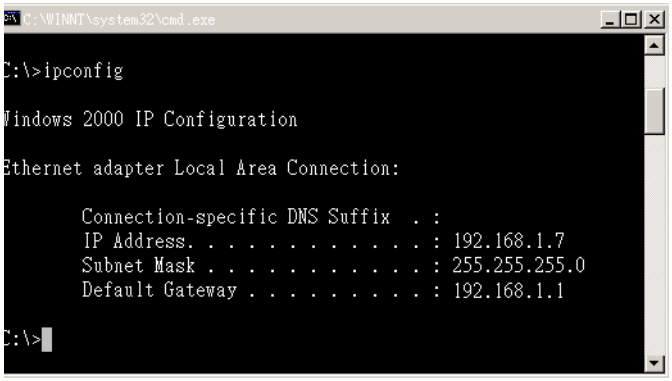
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

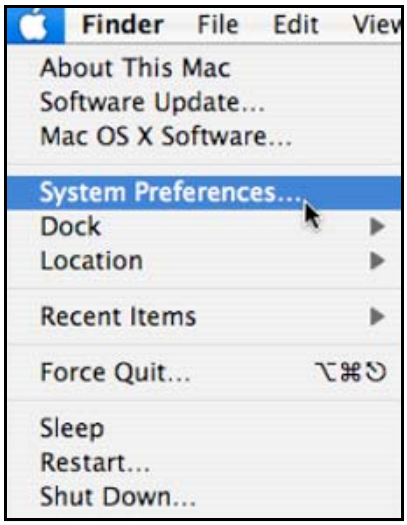
3 The IP settings are displayed as follows.


C:\WINNT\system32\cmd.exe
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.1.7
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\>

Mac OS X: 10.3 and 10.4

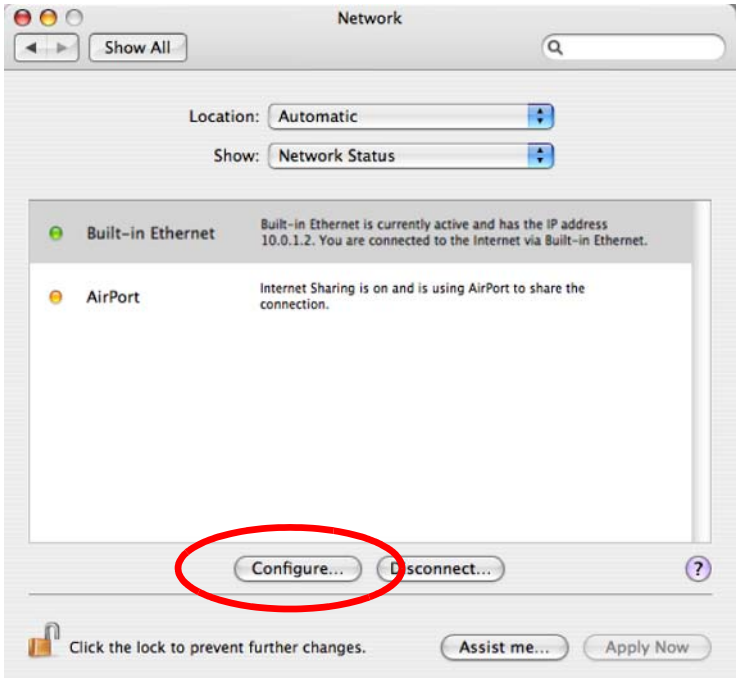
The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

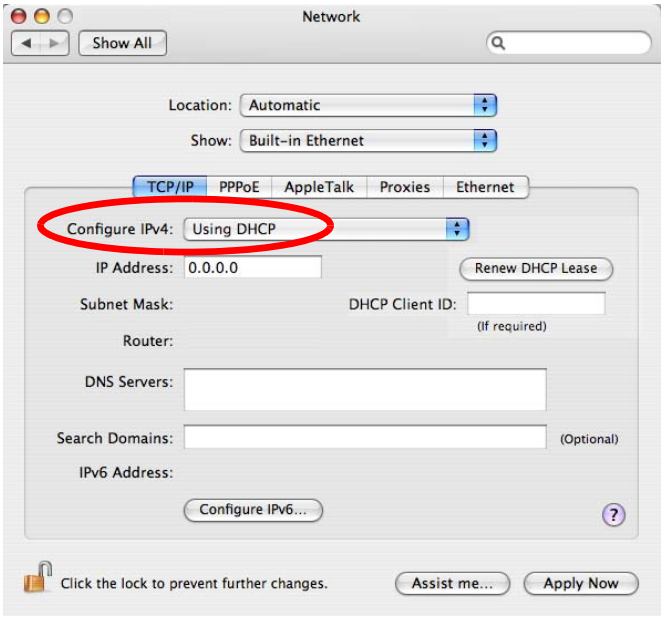


2 In the **System Preferences** window, click the **Network** icon.

3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

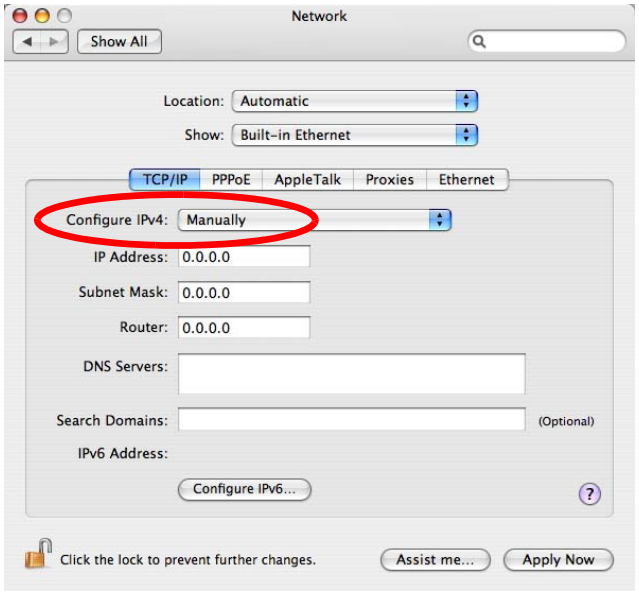

Network
Show All
Location: Automatic
Show: Network Status
Built-in Ethernet
Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.
AirPort
Internet Sharing is on and is using AirPort to share the connection.
Configure...
Disconnect...
Click the lock to prevent further changes.
Assist me...
Apply Now

4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

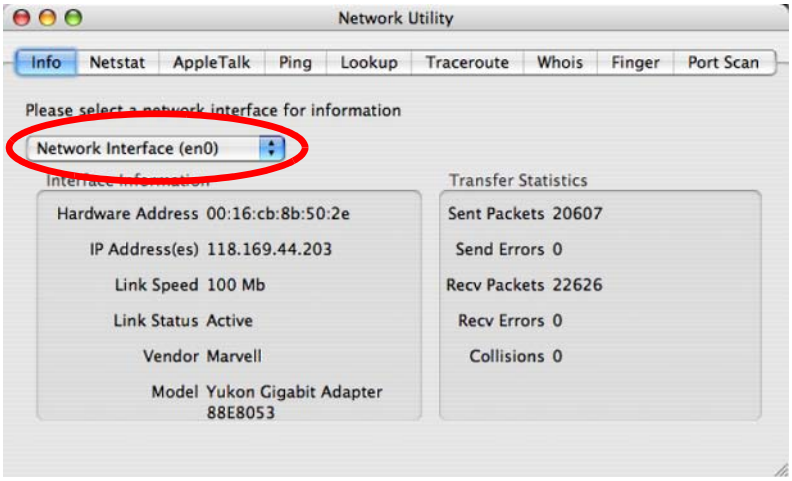


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

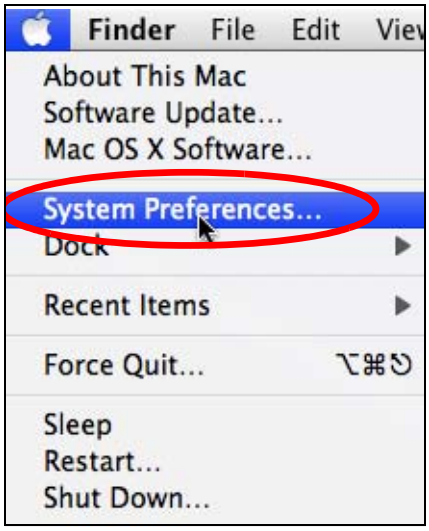
Figure 203 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

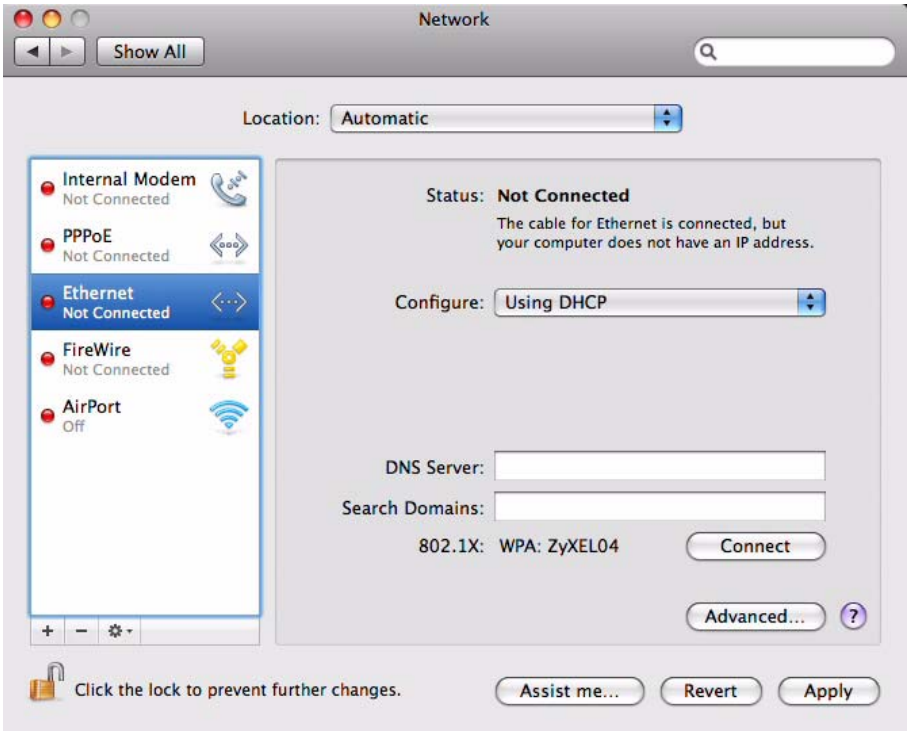
The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

1 Click **Apple** > **System Preferences**.



2 In **System Preferences**, click the **Network** icon.

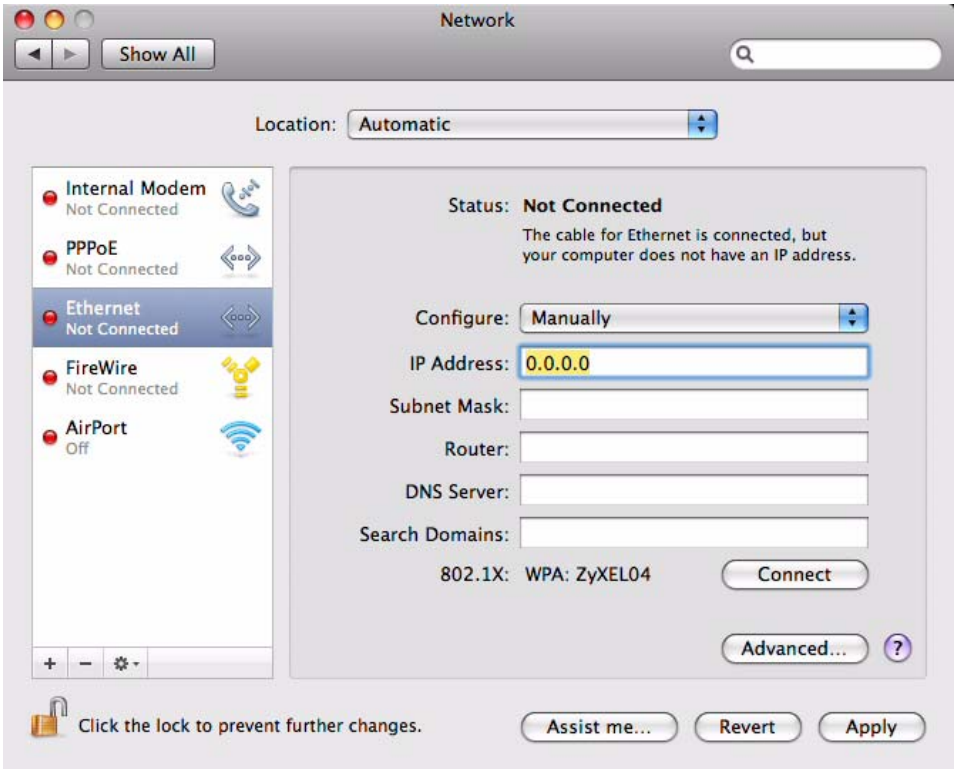
3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your P-2812HNU-51c.

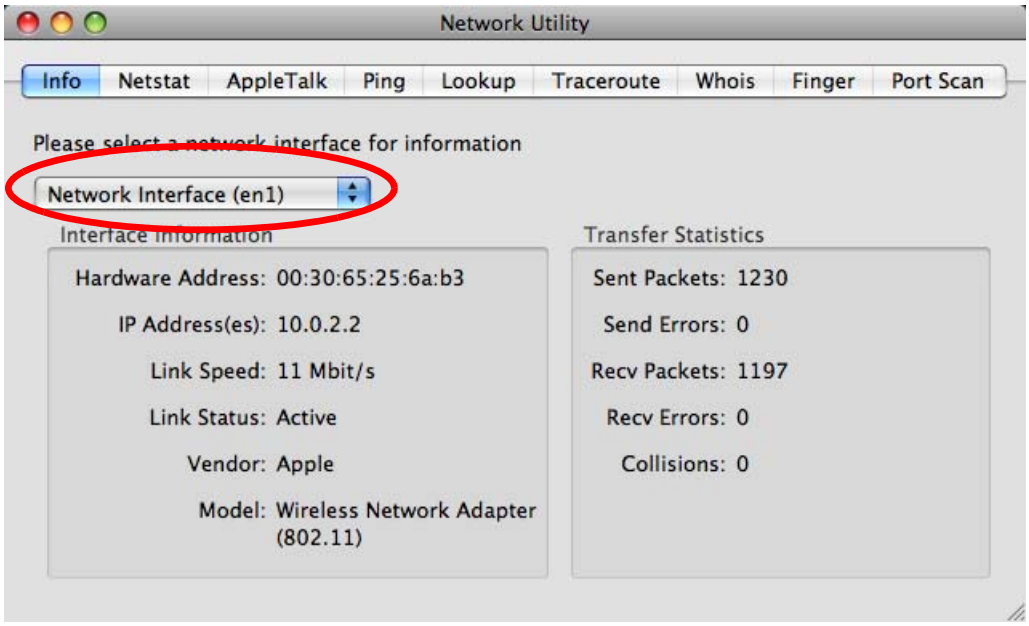


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 204 Mac OS X 10.5: Network Utility



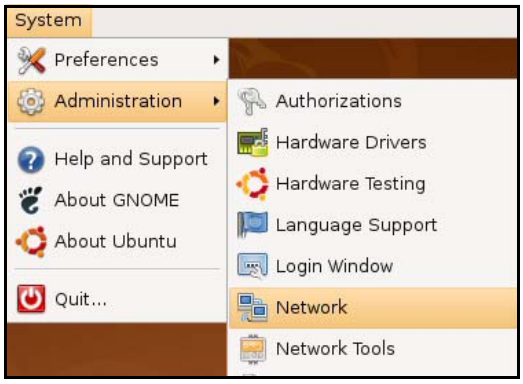
Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

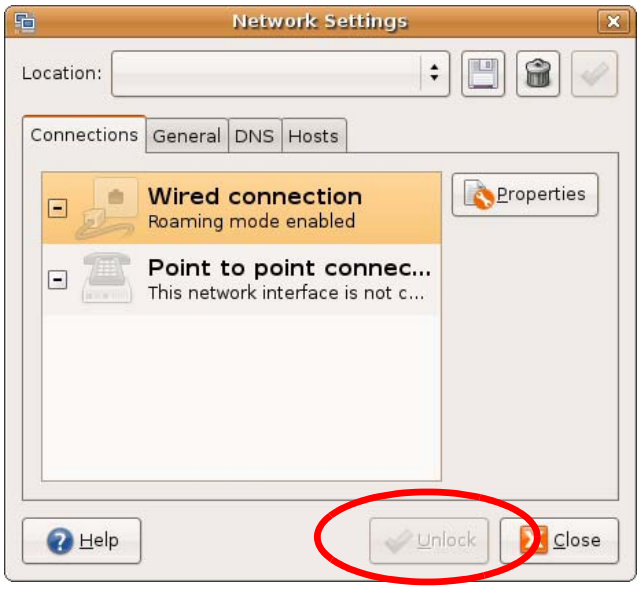
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

1 Click **System > Administration > Network**.



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Authenticate
System policy prevents modifying the configuration
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.
C.J.,,,, (chris)
Password for chris:
Details
Cancel
Authenticate

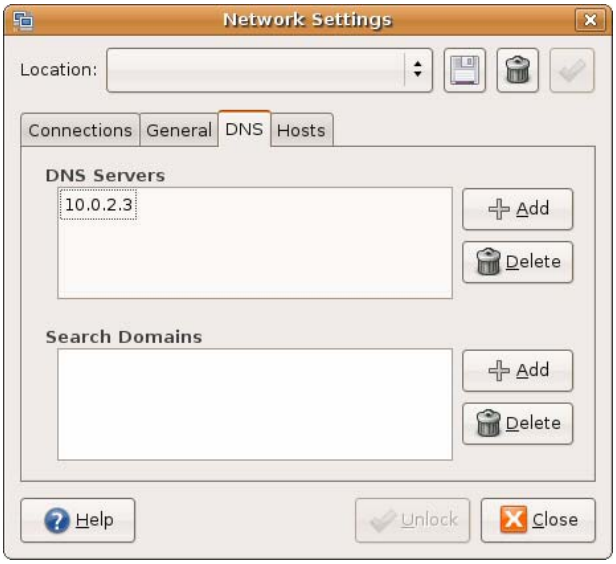
4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

5 The **Properties** dialog box opens.

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

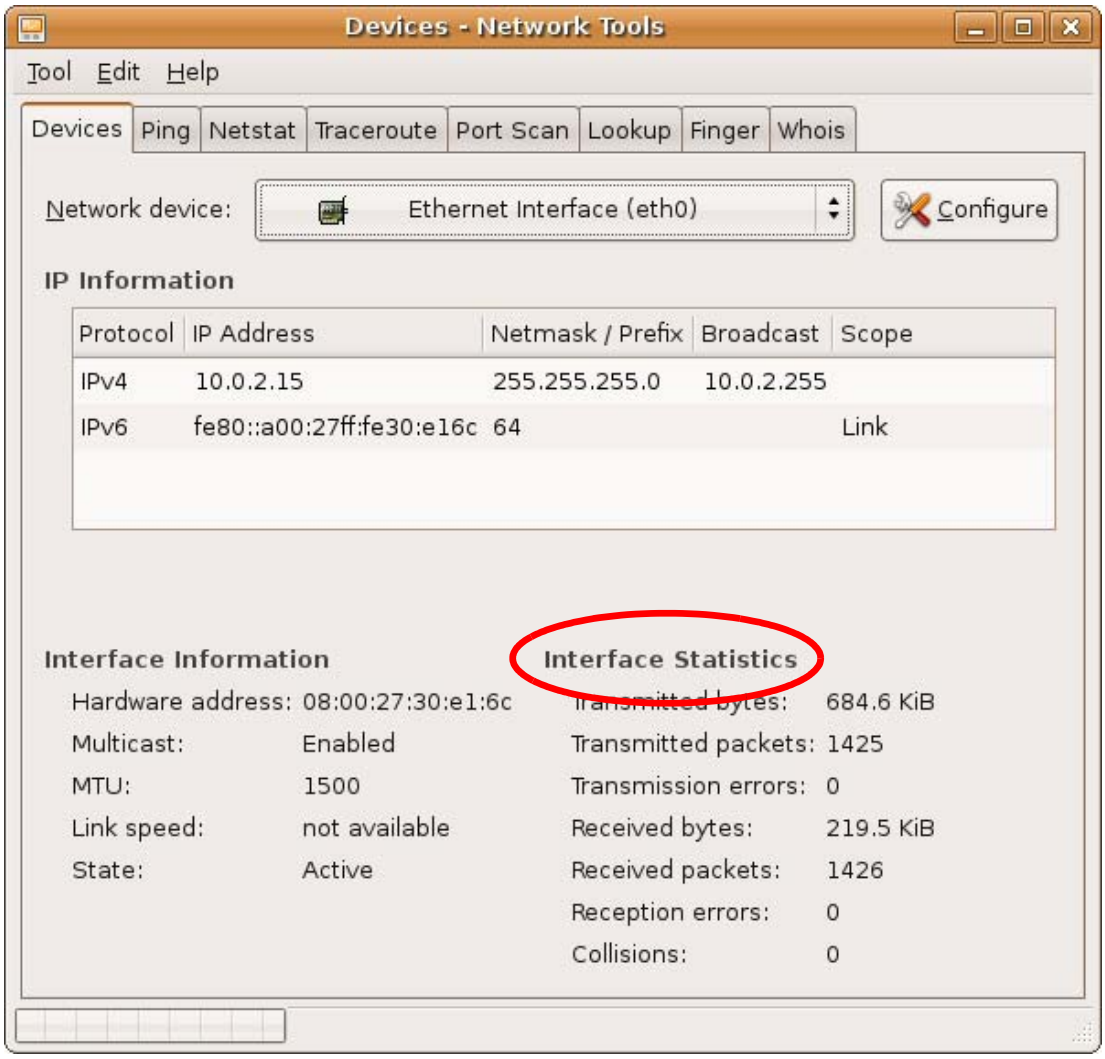


8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 205 Ubuntu 8: Network Tools



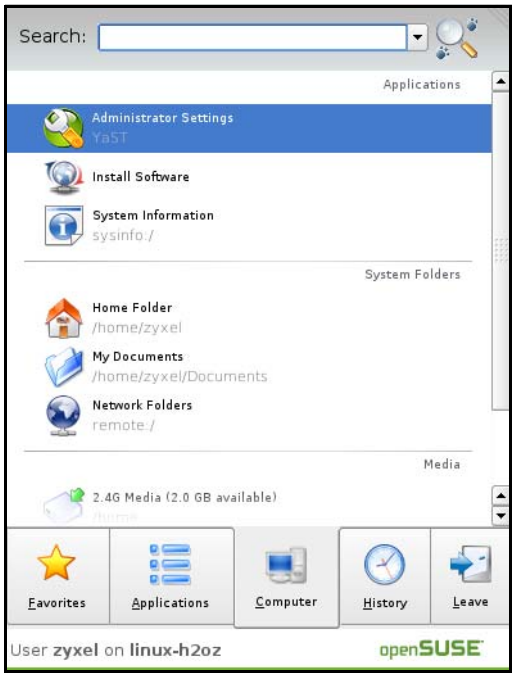
Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

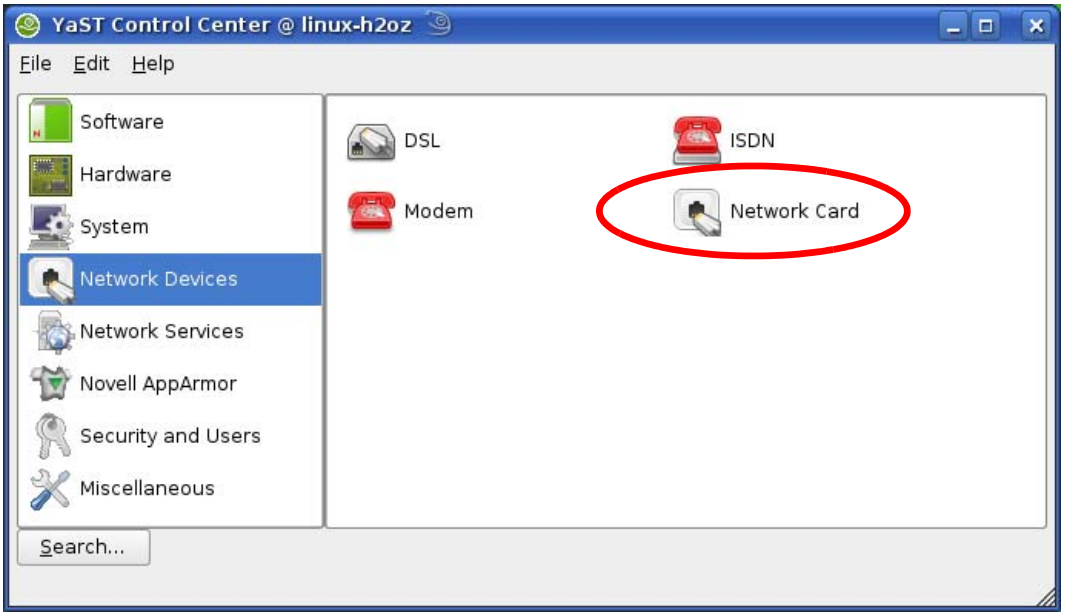
Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu > Computer > Administrator Settings (YaST)**.

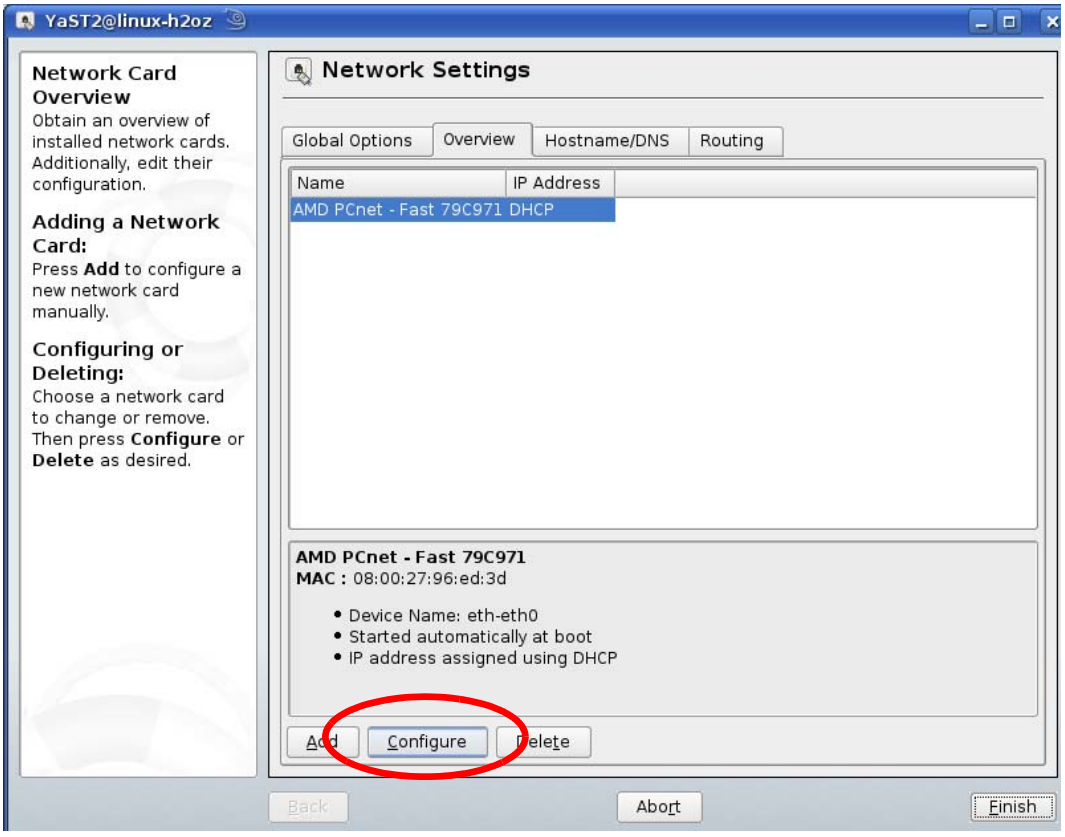


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

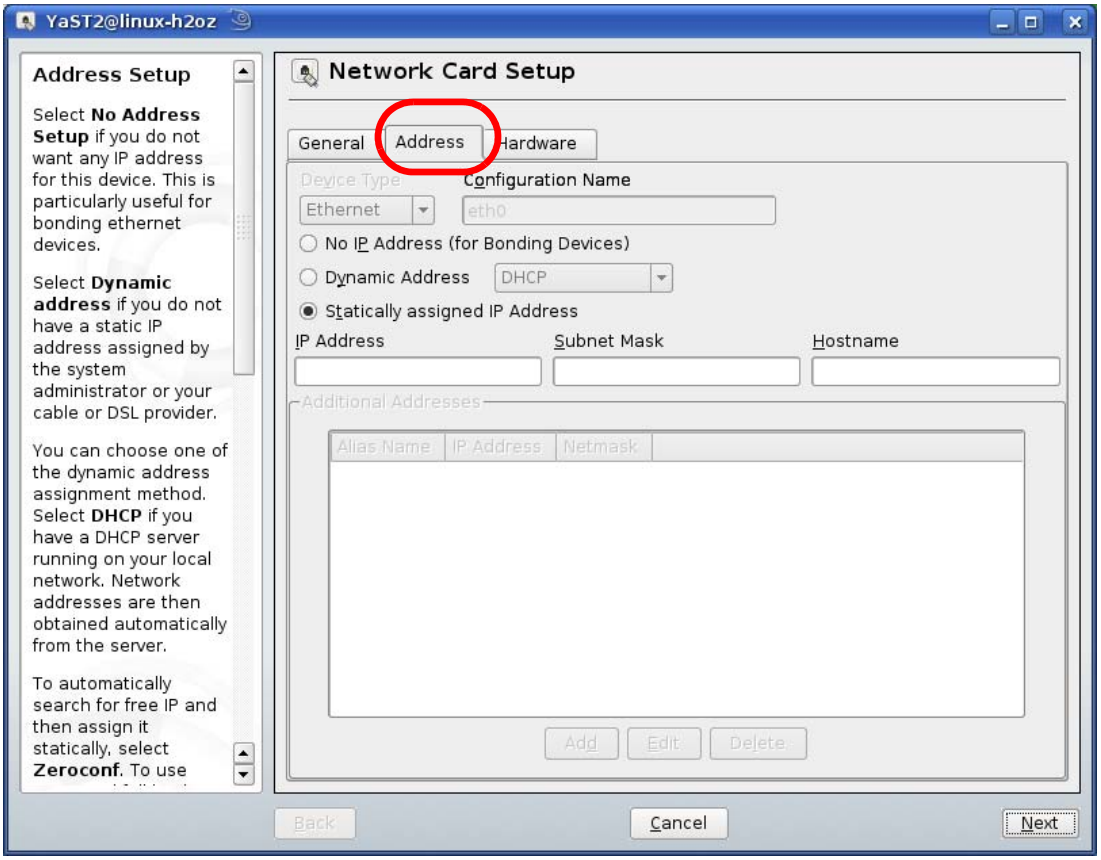


4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 206 openSUSE 10.3: Network Card Setup

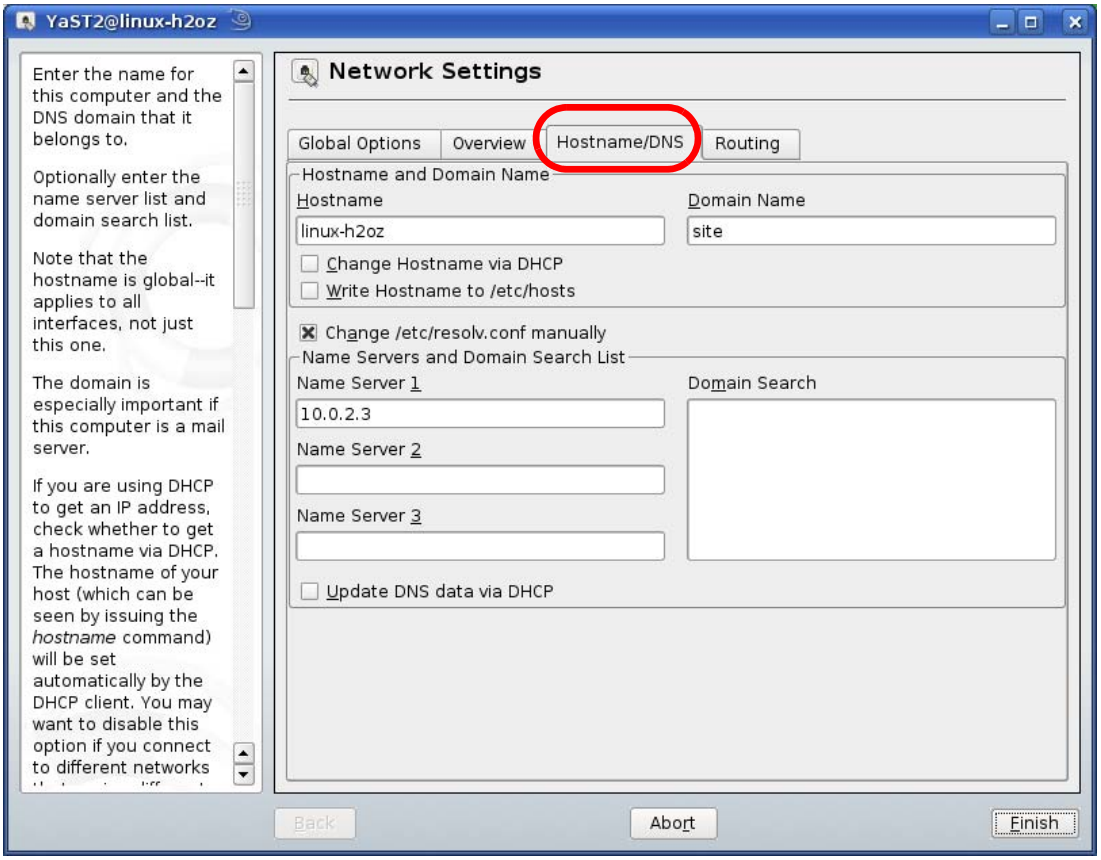

YaST2@linux-h2oz
Address Setup
Select No Address Setup if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.
Select Dynamic address if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.
You can choose one of the dynamic address assignment method. Select DHCP if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.
To automatically search for free IP and then assign it statically, select Zeroconf. To use
Network Card Setup
General
Address
Hardware
Device Type
Configuration Name
Ethernet
eth0
No IP Address (for Bonding Devices)
Dynamic Address
DHCP
Statically assigned IP Address
IP Address
Subnet Mask
Hostname
Additional Addresses
Alias Name
IP Address
Netmask
Add
Edit
Delete
Back
Cancel
Next

6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

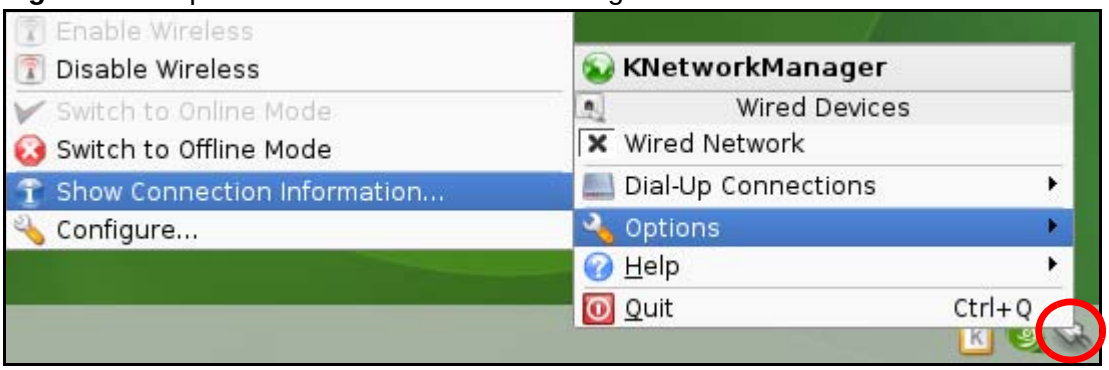

YaST2@linux-h2oz
Enter the name for this computer and the DNS domain that it belongs to.
Optionally enter the name server list and domain search list.
Note that the hostname is global--it applies to all interfaces, not just this one.
The domain is especially important if this computer is a mail server.
If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the hostname command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks
Network Settings
Global Options
Overview
Hostname/DNS
Routing
Hostname and Domain Name
Hostname
linux-h2oz
Domain Name
site
Change Hostname via DHCP
Write Hostname to /etc/hosts
Change /etc/resolv.conf manually
Name Servers and Domain Search List
Name Server 1
10.0.2.3
Domain Search
Name Server 2
Name Server 3
Update DNS data via DHCP
Back
Abort
Finish

9 Click **Finish** to save your settings and close the window.

Verifying Settings

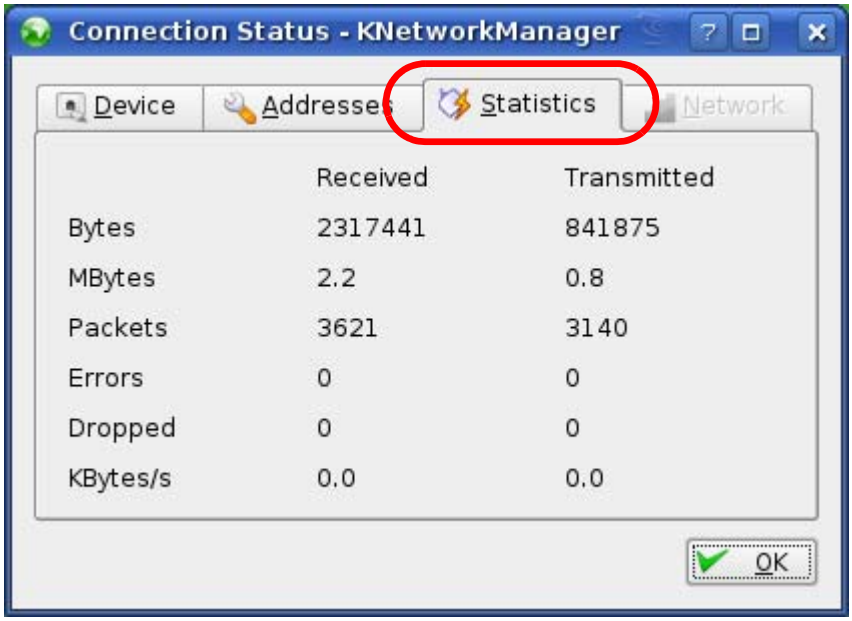
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 207 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 208 openSUSE: Connection Status - KNetwork Manager



C

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

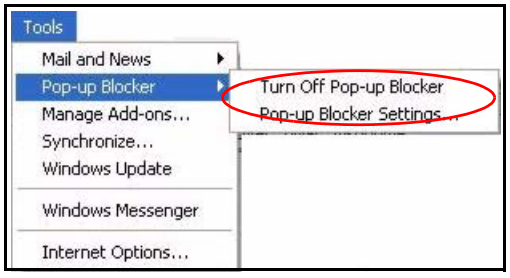
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 209 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 210 Internet Options: Privacy

3 Click **Apply** to save this setting.

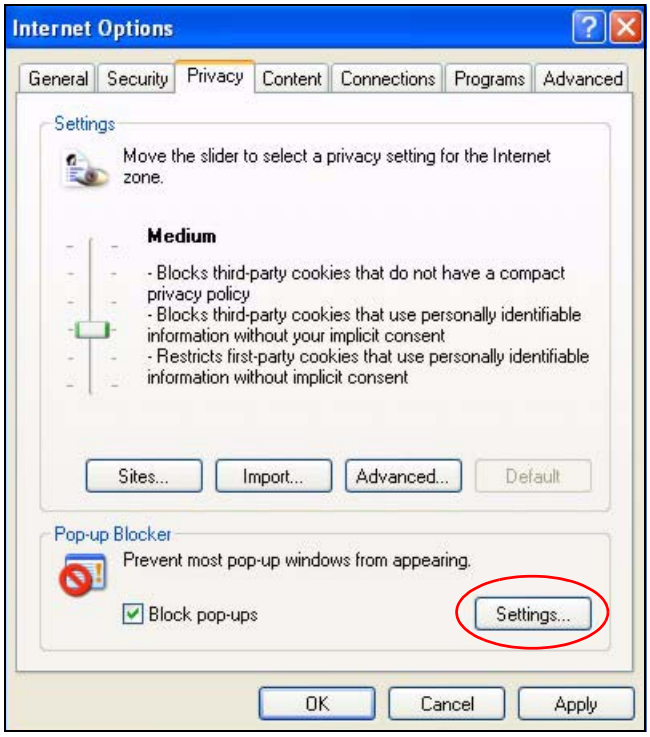
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 211 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 212 Pop-up Blocker Settings

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

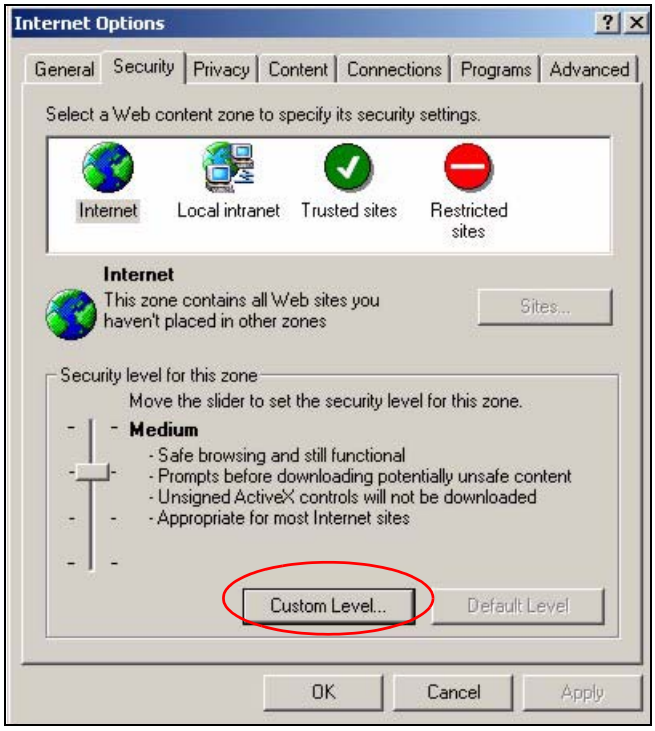
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 213 Internet Options: Security



2 Click the **Custom Level...** button.

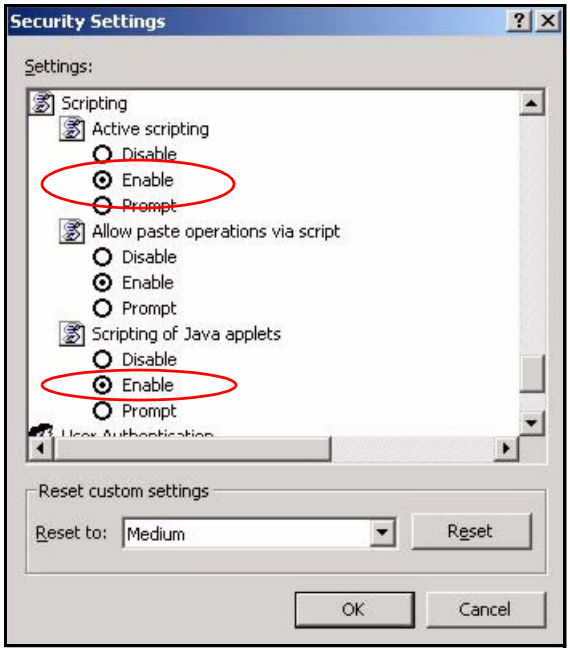
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 214 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

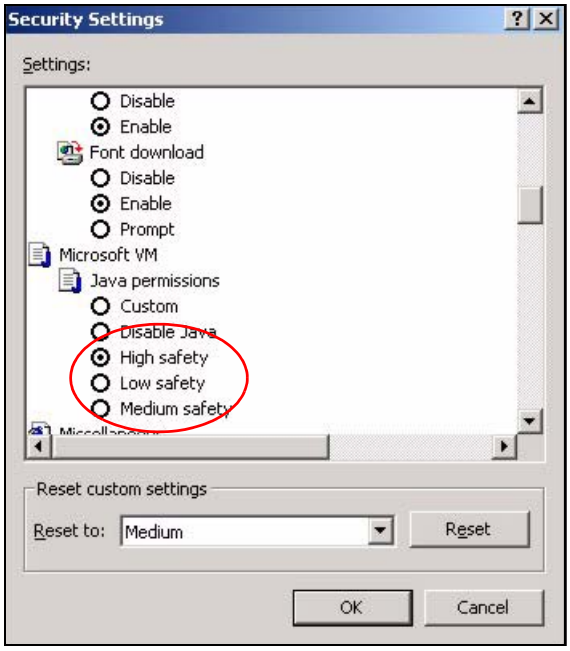
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 215 Security Settings - Java



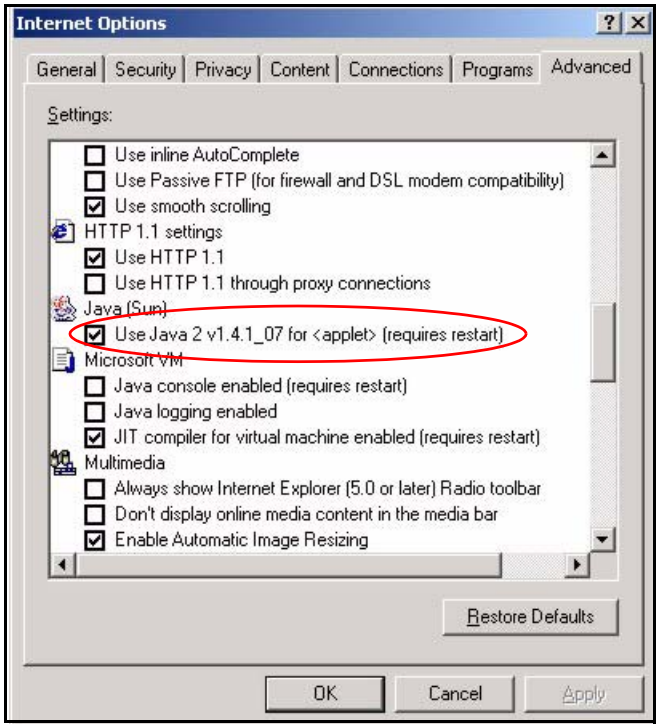
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 216 Java (Sun)

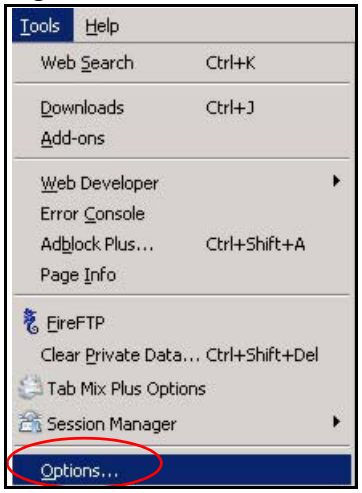


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

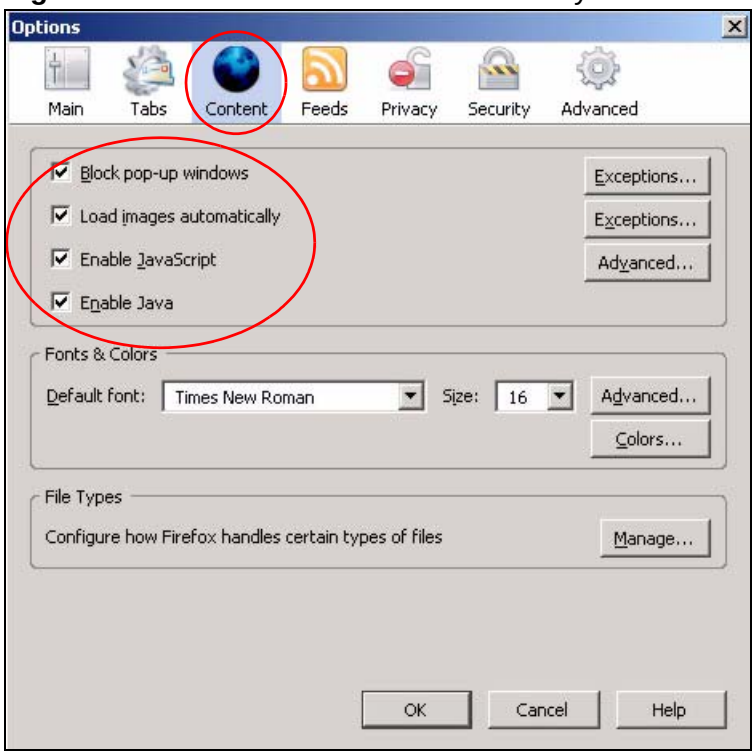
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 217 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 218 Mozilla Firefox Content Security



D

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

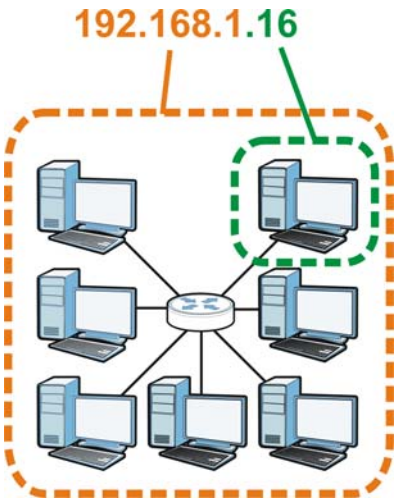
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 219 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 143 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 144 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 145 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 146 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

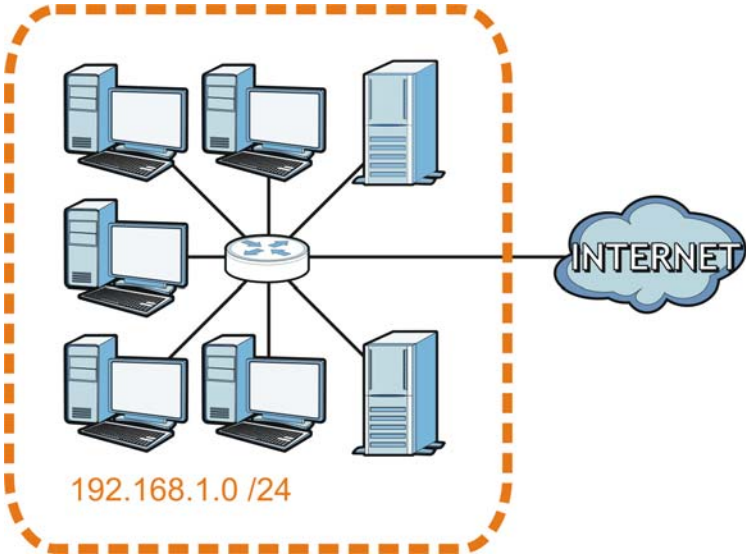
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 220 Subnetting Example: Before Subnetting

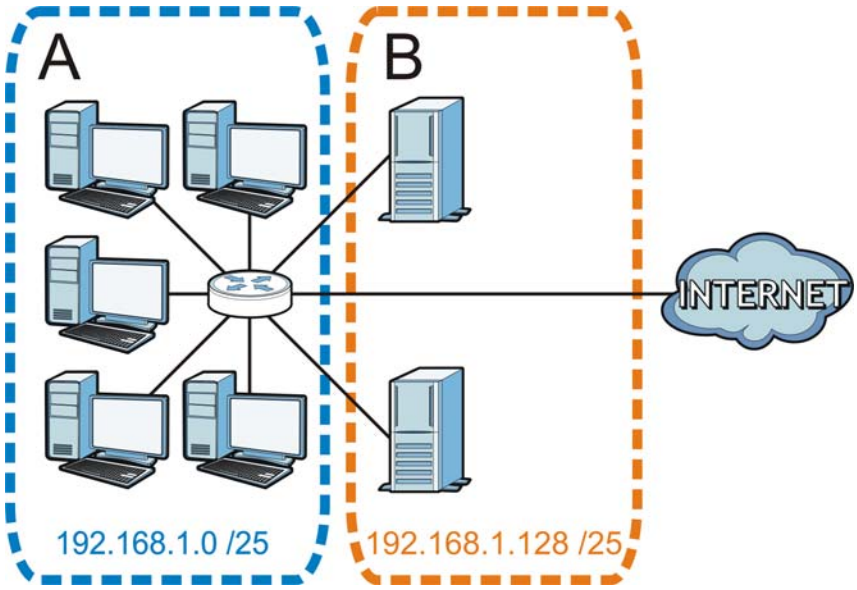


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 221 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 147 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 148 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 149 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 150 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 151 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 152 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 153 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP

addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the P-2812HNU-51c.

Once you have decided on the network number, pick an IP address for your P-2812HNU-51c that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your P-2812HNU-51c will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-2812HNU-51c unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

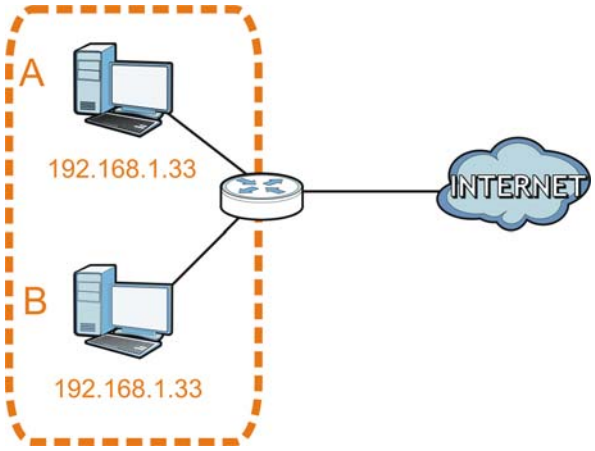
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

Figure 222 Conflicting Computer IP Addresses Example

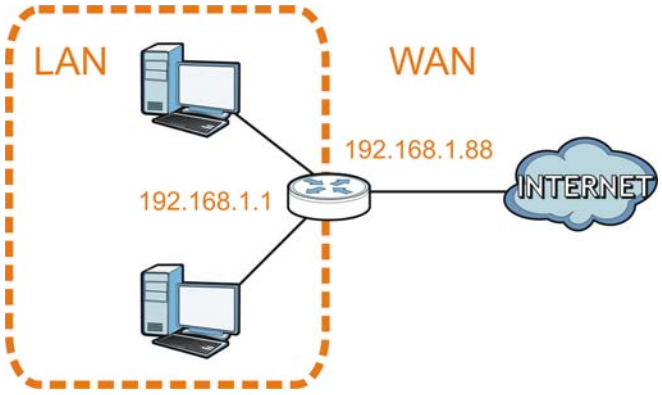


Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the

following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

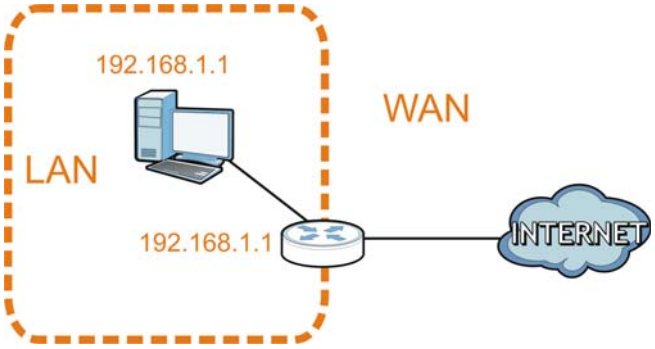
Figure 223 Conflicting Router IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 224 Conflicting Computer and Router IP Addresses Example



E

Wireless LANs

Note: Your specific P-2812HNU-51c may not support all of the wireless security types described in this appendix. See the product specifications for more information about which wireless security types are supported.

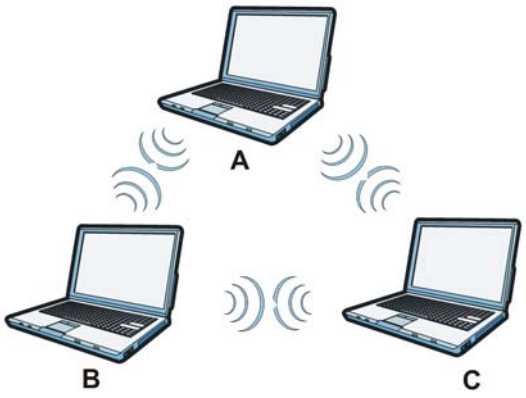
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 225 Peer-to-Peer Communication in an Ad-hoc Network

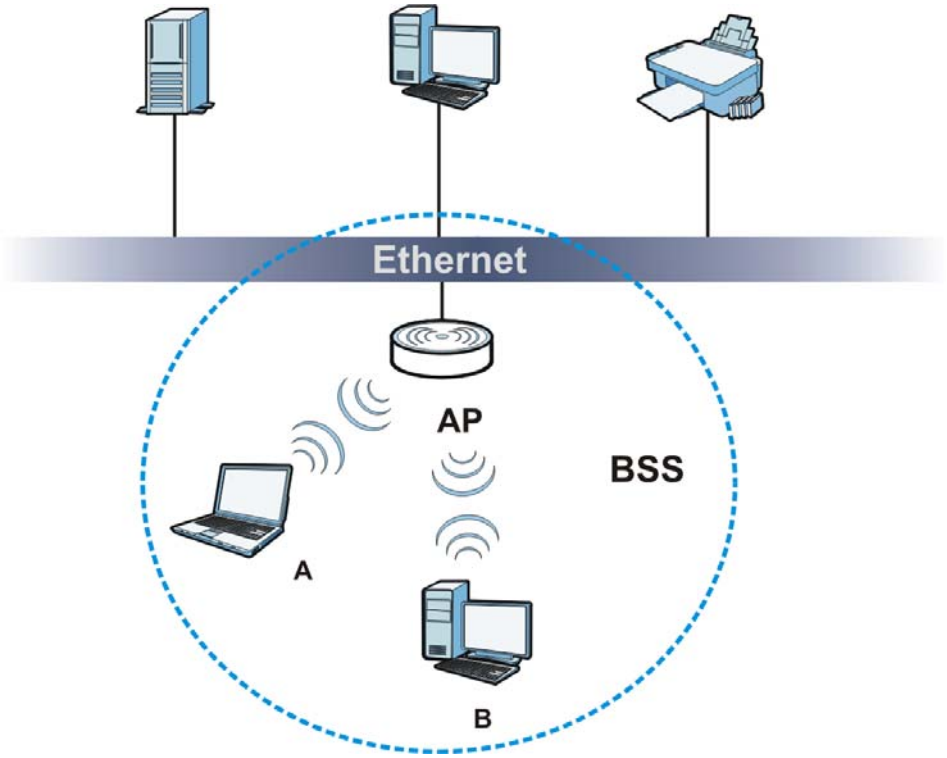


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 226 Basic Service Set



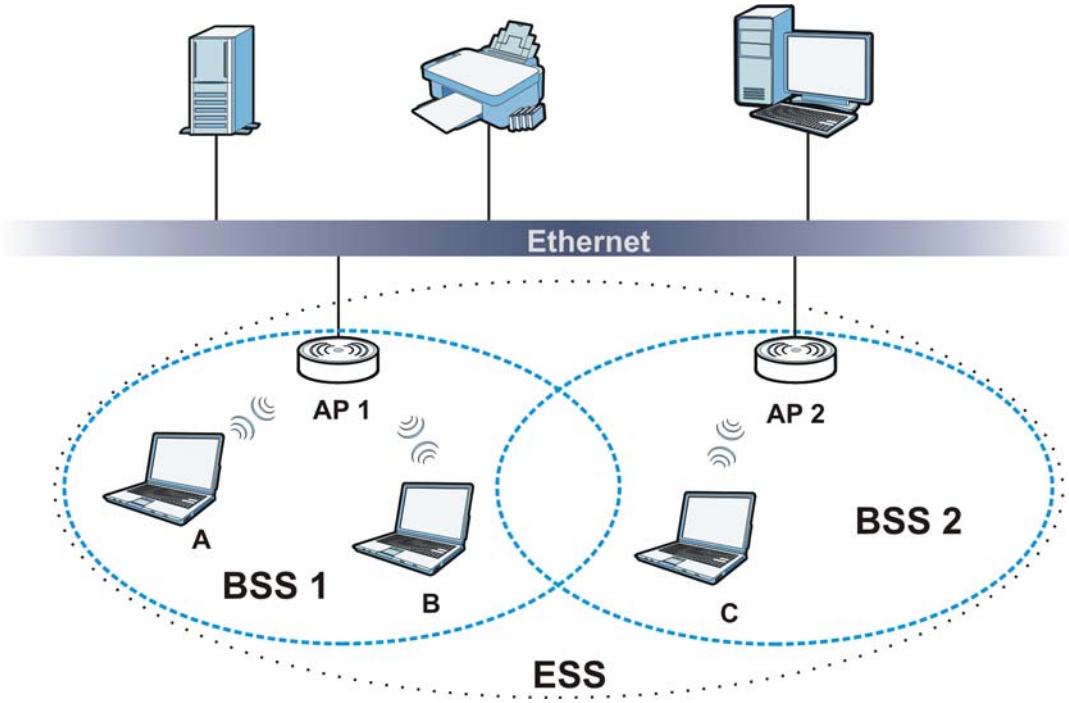
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 227 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

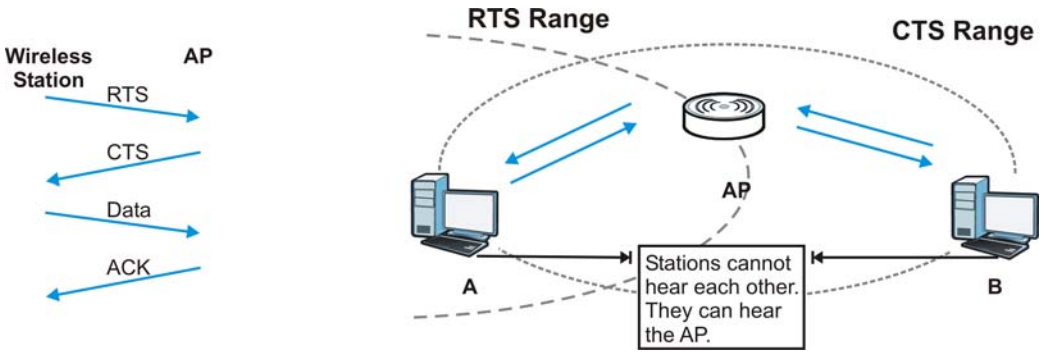
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a

hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 228 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the P-2812HNU-51c uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has

several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 154 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/ 48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the P-2812HNU-51c are data encryption, wireless client authentication, restricting access by device MAC address and hiding the P-2812HNU-51c identity.

The following figure shows the relative effectiveness of these wireless security methods available on your P-2812HNU-51c.

Table 155 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the P-2812HNU-51c and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional

accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5

authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 156 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when

required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-

authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

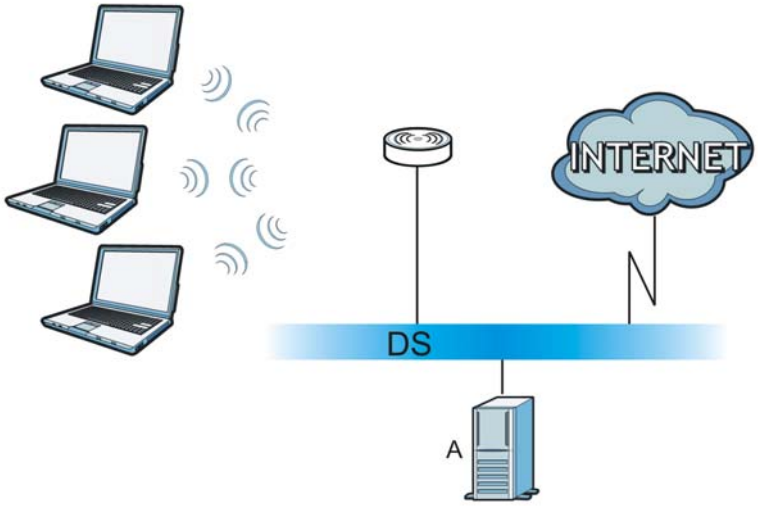
WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 229 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

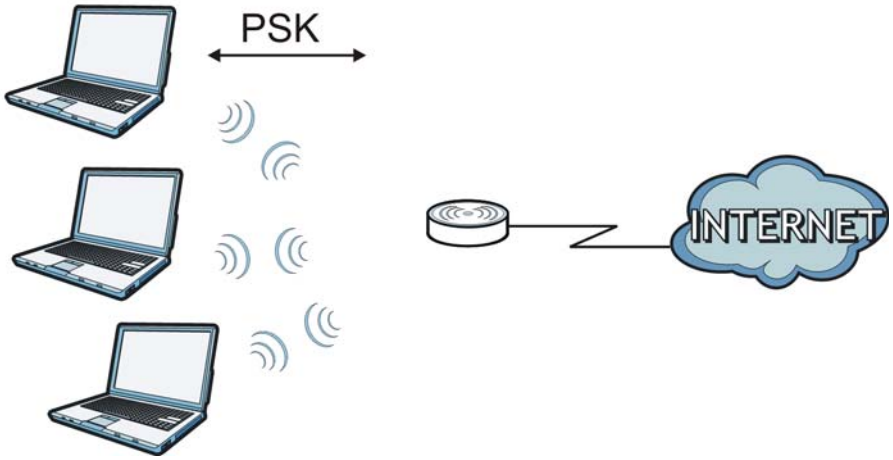
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 230 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 157 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

F

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as “/x” where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 158 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 159 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 160 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

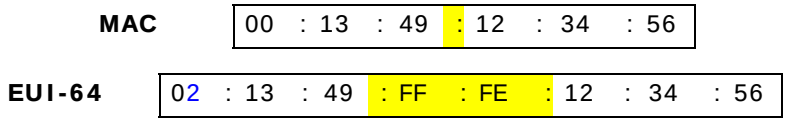
Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the

MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.



Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see Interface ID and EUI-64) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the P-2812HNU-51c is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates [4]another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

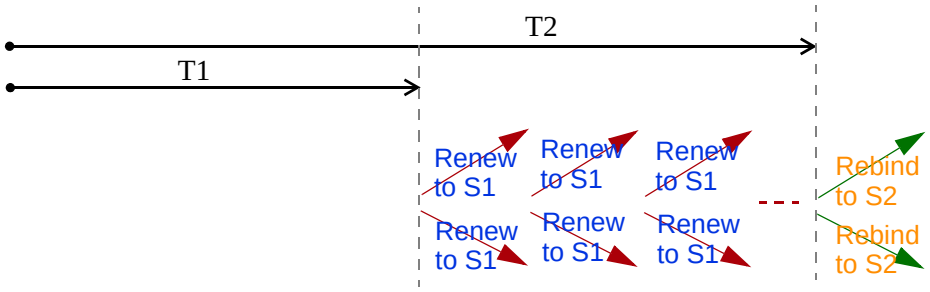
Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses.

4. In IPv6, all network interfaces can be associated with several addresses.

Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The P-2812HNU-51c uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by

multicast, the P-2812HNU-51c passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This

also displays how to use the ipconfig command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the ipconfig command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

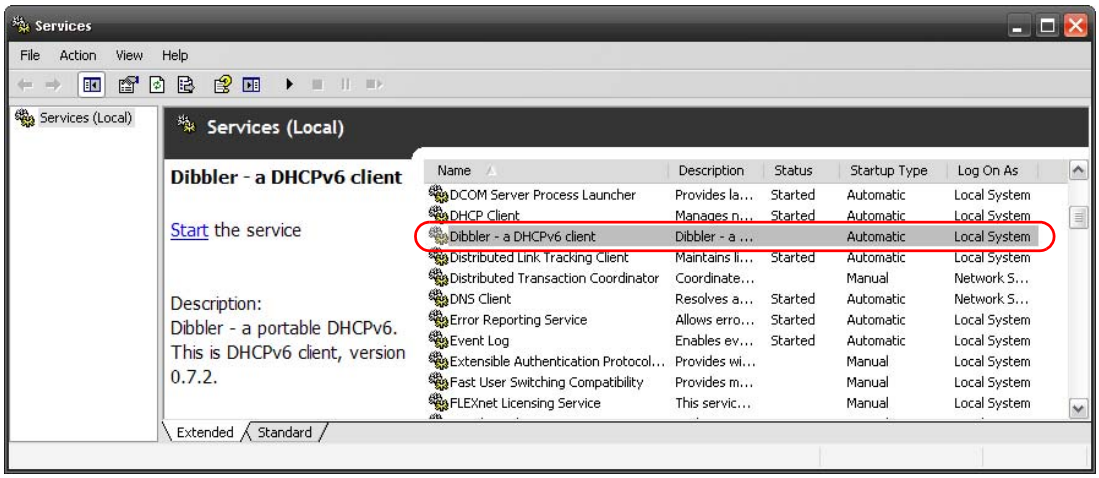
Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

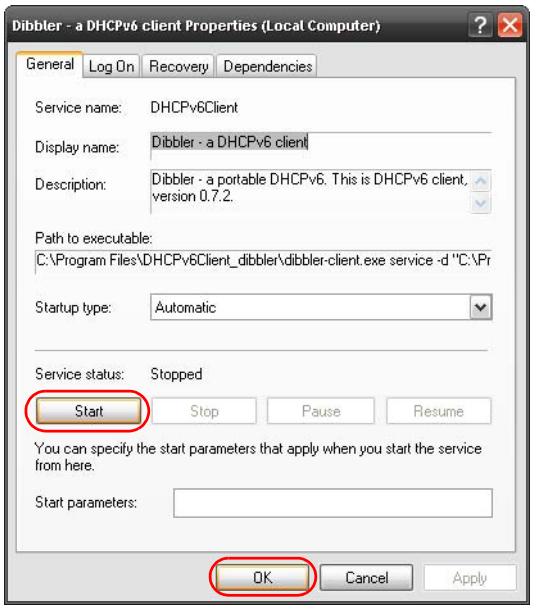
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1. Install Dibbler and select the DHCPv6 client option on your computer.
2. After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.
3. Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.



5 Click **Start** and then **OK**.



6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

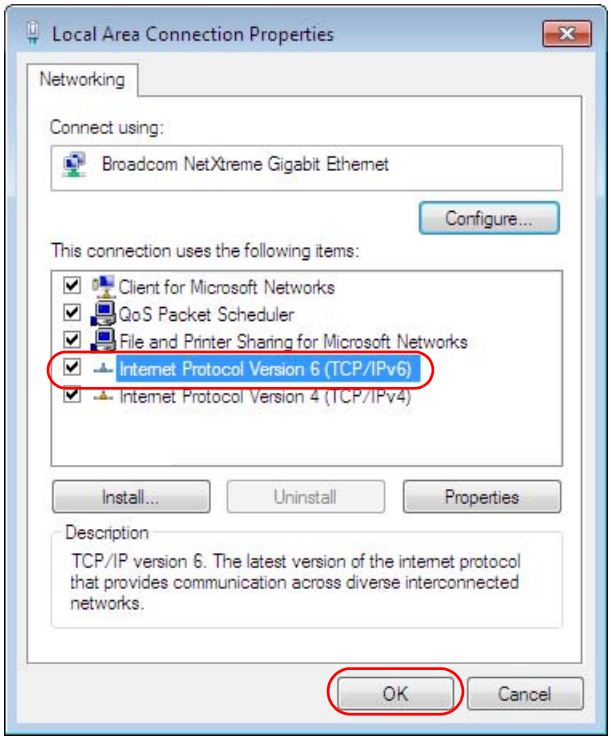
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the ipconfig command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

G

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 161 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.

Table 161 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).

Table 161 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 161 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

H

Open Software Announcements

End-User License Agreement for "P-2812HNU-51c"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED.

1 Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2 Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3 Copyright

The Software and Documentation contain material that is protected by International Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation

4 Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL listed in the below Table (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components, which have been provided on the License Notice as below for the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the Software, and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5 Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms

and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6 No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7 Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8 Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND

DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9 Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10 Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11 General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Note: Some components of this product incorporate source code covered under the open source code licenses. To obtain the source code covered under those Licenses, please check ZyXEL Technical Support (support@zyxel.com.tw) to get it.

Open-Source Packages for "P-2812HNU-51c"

3RD PARTY SOFTWARE	VERSION	WEB ADDRESS OF THE SOFTWARE LICENSE TERM
MIPS Linux kernel	2.6.21.5	http://www.linux-mips.org
Bridge-Utils	1.2	http://bridge.sourceforge.net
bftpd	1.0.24	http://www.bftpd.org/
busybox	1.0.0	http://www.busybox.net/
Dhcpv6		http://sourceforge.net/projects/wide-dhcpv6/
Dnsmasq	2.48	http://www.thekelleys.org.uk/dnsmasq/
Dproxy: dproxy-nexgen		http://dproxy.sourceforge.net
ebtables	2.0.6	http://ebtables.sourceforge.net
iproute2	2.4.7	http://www.linuxgrill.com/anonymous/iproute2
iptables	1.3.8	http://www.netfilter.org
openSSL: openSSL library	0.9.7f	http://www.openssl.org/source/license.html
PPP	2.4.1	http://www.roaringpenguin.com/pppoe
Samba	3.0.34	http://www.samba.org
SSH server: dropbear	0.46	http://matt.ucc.asn.au/dropbear/dropbear.html
Srtp: BSD license	1.4.2	http://srtp.sourceforge.net/srtp.html
Ssmtp: GPLv2	2.62	http://packages.debian.org/lenny/ssmtp
udhcp	0.9.6	http://udhcp.busybox.net/
zebra	0.93a	http://www.zebra.org/

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Bridge-utils 1.2, Busybox 1.0.0, Bftpd 1.0.24, Dnsmasq 2.48, Ebtables 2.0.6, Iproute2 2.4.7, Iptables 1.3.8, MIPS linux kernel 2.6.21.5,

NTFS-3G 1.231, Ppp 2.4.1, Samba 3.0.34, Udhcp 0.9.6 and zebra 0.93a under below GPL license

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to

know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is

normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the

wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE

LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes Ssh server dropbear v0.46 under the MIT-Style License.

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

This Product includes OpenSSL v0.9.7f under the OpenSSL License.

OpenSSL License

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to.

The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR

BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

I

Legal Information

Copyright

Copyright © 2010 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the P-2812HNU-51c is subject to the terms and conditions of any related service providers.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IMPORTANT NOTE

Device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems; users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

注意 !

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

A

AAL5 398
ACK message 221
ACS 331
adding a printer example 242
ADSL2 398
Advanced Encryption Standard
  See AES.
AES 477
AH 268
ALG 192
algorithms 268
alternative subnet mask notation 458
antenna 395
  directional 482
  gain 481
  omni-directional 482
AP (access point) 469
Application Layer Gateway 192
applications
  Internet access 24
arp 409
ATM Adaptation Layer 5 (AAL5) 126
ATM Adaptation Layer 5, see AAL5
Auto Configuration Server, see ACS 331
auto-negotiating rate adaptation 398

B

backup 374
Basic Service Set, See BSS 467
blinking LEDs 31
broadcast 133
BSS 467
BYE request 221

C

CA 281, 475
call history 214
  incoming calls 216
  outgoing calls 215
call hold 228, 230
call service mode 227, 229
call transfer 229, 230
call waiting 228, 230
Canonical Format Indicator See CFI
CBR (Continuous Bit Rate) 104
CCMs 379
certificate
  details 286
  factory default 282
Certificate Authority
  See CA.
certificates 281
  authentication 281
  CA
  creating 283
  importing 284, 288
  public key 281
  replacing 282
  storage space 282
Certification Authority 281
Certification Authority. see CA
certifications 511
  notices 513
  viewing 514
CFI 133
CFM 379
  CCMs 379
  link trace test 380
  loopback test 380
  MA 379
  MD 379
  MEP 379
  MIP 379
channel 469

interference 469
channel ID 153
CIFS 234
CIFS (Common Internet File System) 236
Class of Service 226
Class of Service, see CoS
client-server protocol 218
comfort noise generation 224
command parameters 402
command syntax 402
Common Internet File System (CIFS) 236
Common Internet File System, see CIFS
configuration 138, 144
Connectivity Check Messages, see CCMs
copyright 511
CoS 226, 325
CoS technologies 308
CPU usage 84
creating certificates 283
CTS (Clear to Send) 470

D

date and time 84
default 376
default LAN IP address 73
DH 274
DHCP 96, 138, 144, 329
DHCP client 96
DHCP client list 96
DHCP relay 396
DHCP server 396
diagnostic 380, 383
differentiated services 226
Differentiated Services, see DiffServ 325
Diffie-Hellman key groups 274
DiffServ 325
marking rule 325
DiffServ (Differentiated Services) 226
code points 226
marking rule 226
digital IDs 281
disclaimer 511
DNS 139
DNS server address assignment 133
Domain Name 193
domain name system
see DNS
Domain Name System. See DNS.
DS field 226, 325
DS, dee differentiated services
DSCP 226, 325
DSL interface 99
dynamic DNS 329
Dynamic Host Configuration Protocol. See DHCP.
dynamic WEP key exchange 475
DYNDNS wildcard 329

E

EAP Authentication 474
ECHO 193
echo cancellation 224
Encapsulation 125
MER 125
PPP over Ethernet 125
PPPoA 126
encapsulation 268
RFC 1483 126
encryption 476
WEP 157
end-to-end loopback test 383
ESP 268
ESS 468
ESSID 84
Europe type call service mode 227
Extended Service Set IDentification 154
Extended Service Set, See ESS 468

F

F4 cells 383
F4/F5 OAM 398

F5 cells 383
FCC interference statement 511
file sharing 27, 236
Finger 193
firmware
  upload 372
  upload error 373
firmware version 83
flash key 227
flashing 227
fragmentation threshold 471
FTP 184, 193

G

G.168 224
G.992.3 398
G.992.4 398
G.992.5 398

H

hidden node 469
host 364
host name 83
HTTP 193, 275, 276
HTTP (Hypertext Transfer Protocol) 372
humidity 395

I

IANA 145, 463
IBSS 467
ID type and content 272
IEEE 802.11g 471
IEEE 802.1Q 132
IGMP 133, 138, 146
  version 133
IGMP proxy 398
IGMP v1 398
IGMP v2 398
IKE phases 269
importing certificates 284, 288
Independent Basic Service Set
  See IBSS 467
initialization vector (IV) 477
inside header 269
Integrated Access Device 23
internal routing table 90
Internet access 24
Internet Assigned Numbers Authority
  See IANA 463
Internet Key Exchange 269
Internet Protocol Security, see IPSec
Internet Protocol version 6, see IPv6
IP Address 192
IP address 144
IP Address Assignment 128
IP filter
  basics 275
  creating or eiding rules 278
  introduction 275
  policies 276
IP multicasting 398
IP pool 140
IP pool setup 144
ipconfig 403
ipconfig, release 404
ipconfig, renew 404
IPSec 253
  algorithms 268
  architecture 267
  NAT 270
  see also VPN
IPv6 100, 483
  addressing 483
  EUI-64 485
  global address 484
  interface ID 485
  link-local address 484
  Neighbor Discovery Protocol 100, 483
  ping 100, 483
  prefix 483
  prefix length 483
  stateless autoconfiguration 486
  unspecified address 484

ITU-T 224

K

key combinations 231
keypad 231

L

LAN
and USB printer 240
LAN statistics 95
LAN TCP/IP 144
LAN-Side DSL CPE Configuration 333
LBR 380
link trace 380
Link Trace Message, see LTM
Link Trace Response, see LTR
listening port 206
logs 367
overview 367
settings 368
Loop Back Response, see LBR
loopback 380
LTM 380
LTR 380

M

MA 379
MAC 83
MAC address 83
MAC address filter action 161
MAC filter 160, 161
Maintenance Association, see MA
Maintenance Domain, see MD
Maintenance End Point, see MEP
Management Information Base (MIB) 334
managing the device
good habits 24
Maximum Burst Size (MBS) 105, 127
MD 379
memory usage 85
MEP 379
Message Integrity Check (MIC) 476
MIB
and SNMP 334
MIB (Management Information Base) 334
MTU (Multi-Tenant Unit) 132
multicast 133, 138, 146
multimedia 217
multiplexing 126
LLC-based 127
VC-based 126
multiprotocol encapsulation 126

N

NAT 145, 183, 463
default server 192
DMZ host 192
external port 185
internal port 185
IPSec 270
port forwarding 184
port number 184, 193
services 193
Symmetric 131
traversal 271
NAT example 194
NAT Types 129
negotiation mode 270
netstat 413
Network Address Translation, see NAT
network troubleshooting 401
arp 409
ipconfig 403
netstat 413
ping 405
route 410
tracert 407
NNTP 193
non-proxy calls 212

O

OAM 383, 398
OAM ping test 383
OK response 221, 223
operation humidity 395
operation temperature 395
Operation, Administration and Maintenance, see OAM
outside header 269

P

Packet Transfer Mode 99
Pairwise Master Key (PMK) 477, 479
Peak Cell Rate (PCR) 105, 127
peer-to-peer calls 212
Per-Hop Behavior, see PHB 325
PHB 226, 325
phone book
  speed dial 212
phone functions 231
ping 405
  timeout 406
Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) 126
Point-to-Point Tunneling Protocol 194
POP3 193, 275, 276
ports 31
power adaptor 399
power specifications 395
PPP (Point-to-Point Protocol) Link Layer Protocol 398
PPP over ATM AAL5 398
PPP over Ethernet 398
PPPoE 126
  Benefits 126
PPPoE (Point-to-Point Protocol over Ethernet) 397
PPTP 194
preamble mode 471
pre-shared key 274
print server 27
printer sharing 239
  and LAN 240
  requirements 240
product registration 514
PSK 477
PTM 99

Q

QoS 225, 307, 325
  marking 308
  setup 307
  tagging 308
  versus CoS 308
Quality of Service, see QoS
Quick Start Guide 73

R

RADIUS 473
  message types 473
  messages 473
  shared secret key 474
Reach-Extended ADSL 398
Real time Transport Protocol, see RTP
registration
  product 514
related documentation 3
remote management
  TR-069 331
Remote Procedure Calls, see RPCs 331
resetting your device 29
restore 375
RFC 1058. See RIP.
RFC 1389. See RIP.
RFC 1483 126, 398
RFC 1631 183
RFC 1889 220
RFC 2131. See DHCP.
RFC 2132. See DHCP
RFC 2364 398
RFC 2516 397, 398

RFC 2684 398
RIP 138, 305
Routing Information Protocol
see RIP
route 410
route status 91
router features 24
routing information 90
Routing Information Protocol. See RIP
RPPCs 331
RTP 220
RTS (Request To Send) 470
threshold 469, 470

S

safety warnings 7
seamless rate adaptation 398
secure gateway address 254
security associations, see VPN
Security Parameter Index 261
segment loopback test 383
service access control 336
Service Set 154
Services 193
Session Initiation Protocol, see SIP
sharing files 236
silence suppression 224
Simple Network Management Protocol, see SNMP
Single Rate Three Color Marker, see srTCM
SIP 217
account 217
call progression 221
client 218
identities 217
INVITE request 221, 223
number 217
OK response 223
proxy server 219
redirect server 219
register server 220
servers 218
service domain 217
URI 217
user agent 218
SIP ALG 192
SIP Application Layer Gateway 192
SMTP 193
SNMP 193, 334, 398
agent 334
and MIB 334
manager 334
network components 334
object variables 334
protocol operations 334
SNMP trap 194
speed dial 212
SPI 261
SRA 398
srTCM 327
static route 293, 297, 301, 305, 359
static VLAN
status indicators 31
storage humidity 395
storage temperature 395
subnet 455
subnet mask 144, 456
subnetting 458
supplementary services 227
Sustain Cell Rate (SCR) 105
Sustained Cell Rate (SCR) 127
Symmetric NAT 131
Symmetric NAT, Outgoing 132
syntax conventions 5
system name 83

T

Tag Control Information See TCI
Tag Protocol Identifier See TPID
TCI
TCP/IP 275
temperature 395
Temporal Key Integrity Protocol (TKIP) 476
three-way conference 229, 230
ToS 226

TPID 132
TR-064 333
TR-069 331
  ACS setup 331
  authentication 332
tracert 407
trademarks 511
traffic shaping 127
transparent bridging 398
transport mode 268
trTCM 328
tunnel mode 269
Two Rate Three Color Marker, see trTCM
Type of Service, see ToS

U

unicast 133
Uniform Resource Identifier 217
Universal Plug and Play 339
  application 340
UPnP 339
  cautions 340
  forum 340
  NAT traversal 339
  security issues 340
USA type call service mode 229
USB
  printer sharing 239
USB features 27
USB printer 27

V

VAD 224
VCI 383
VID
virtual channel 383
Virtual Circuit (VC) 126
virtual circuits 383
  terminology 383
Virtual Local Area Network See VLAN
virtual path 383
Virtual Private Network, see VPN
VLAN 132
  Introduction 132
  number of possible VIDs
  priority frame
  static
VLAN ID 132
VLAN Identifier See VID
VLAN tag 132
voice activity detection 224
voice coding 223
VoIP 217
  peer-to-peer calls 212
VoIP features 27
VPI 383
VPN 253
  established in two phases 254
  IPSec 253
  security associations (SA) 254
  see also IKE SA, IPSec SA

W

WAN (Wide Area Network) 97
WAN interface 89
WAN statistics 89
warranty 514
  note 514
Web Configurator 73
WEP encryption 158
Wi-Fi Protected Access 476
Windows Command Prompt 402
  arp 409
  command parameters 402
  ipconfig 403
  netstat 413
  ping 405
  route 410
  tracert 407
wireless client WPA supplicants 478
wireless security 472
wireless station list 94
Wireless tutorial 33

WLAN
interference 469
security parameters 480
WLAN button 28
WPA 476
key caching 478
pre-authentication 478
user authentication 477
vs WPA-PSK 477
wireless client supplicant 478
with RADIUS application example 478
WPA2 476
user authentication 477
vs WPA2-PSK 477
wireless client supplicant 478
with RADIUS application example 478
WPA2-Pre-Shared Key 476
WPA2-PSK 476, 477
application example 479
WPA-PSK 476, 477
application example 479
WPS
status 84